



Panic Alarm Station

User Manual

User Manual

COPYRIGHT ©2018 Hangzhou Hikvision Digital Technology Co., Ltd.

ALL RIGHTS RESERVED.

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be "Hikvision"). This user manual (hereinafter referred to be "the Manual") cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

About this Manual

This Manual is applicable to panic alarm station.

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 in the company website (http://overseas.hikvision.com/en/).

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

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

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED "AS IS", WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS 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 OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITES 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.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

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

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC Compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- -Reorient or relocate the receiving antenna.
- -Increase the separation between the equipment and receiver.
- -Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- -Consult the dealer or an experienced radio/TV technician for help

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: 1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation. **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, LVD Directive 2014/35/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

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

Applicable Models

Product	Model
Panic Alarm Station	DS-PEA1-21
Box Panic Alarm Station	DS-PEA2-21
Pole Panic Alarm Station	DS-PEA3M-21 DS-PEA3M-21H

This manual is applicable to the models listed in the following table.

Symbol Conventions

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

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

Safety Instruction



- The device should be used in compliance with local laws and electrical safety regulations. Refer to the appropriate documentation for detailed information.
- The input voltage should conform to IEC60950-1 standard: SELV (Safety Extra Low Voltage) and the Limited Power Source (100~120/200~240 VAC). Refer to the appropriate documentation for detailed information.
- DO NOT connect multiple devices to one power adapter, to avoid over-heating or fire hazards caused by overload.
- Make sure the plug is properly connected to the power socket.
- If smoke, odor, or noise arises from the device, immediately turn off the power, unplug the power cable, and contact the service center.

- Do not drop the device or subject it to physical shock.
- Wipe the device gently with a clean cloth and a small quantity of ethanol, if necessary.
- Do not aim the lens at the sun or any other bright light.

- When any laser equipment is in use, make sure that the device lens is not exposed to the laser beam, or it may burn out.
 - Do not expose the device to high electromagnetic radiation or extremely hot, cold, dusty, or damp environments, the appropriate temperature is -40° C to 60° C.
- Place the device in a dry and well-ventilated environment.
- Keep non-waterproof devices away from liquids.
- Keep the device in original or similar packaging while transporting it.
- A few device components (e.g., electrolytic capacitor) require regular replacement. The average lifespan varies, so periodic checking is recommended. Contact your dealer for details.
- Improper use or replacement of the battery may result in explosion hazard. Replace with the same or equivalent type only. Dispose of used batteries in conformance with the instructions provided by the battery manufacturer.
- Never attempt to disassemble the device.

Table of Content

Chapter 1 Overview	6
1.1 Description	6
1.2 Key Features	6
Chapter 2 Structure Description	7
2.1 Mainboard Description	7
2.2 Appearance Description	8
2.2.1 Panic Alarm Station	8
2.2.2 Box Panic Alarm Station	9
2.2.3 Pole Panic Alarm Station	10
2.3 Installation and Connections	10
2.3.1 Power Supply Wiring	11
2.3.2 Network Wiring	11
2.3.3 Audible and Visual Alarm Wiring	12
2.3.4 Alarm Input Wiring (Normally Open)	12
2.3.5 Pole Panic Alarm Station Installation	13
Chapter 3 Activating the Control Panel	17
Chapter 4 Device Remote Operation	18
4.1 Device Management	18
4.1.1 Add a Device	18
4.1.2 Edit a Device	19
4.1.3 Delete a Device	19
4.1.4 Status	20
4.2 Remote Configurations	20
4.2.1 System Information Settings	20
4.2.2 Network Settings	26
4.2.3 Storage	31
4.2.4 Alarm Settings	33
4.2.5 Image Settings	37
4.2.6 Event Settings	39
4.2.7 Operation	40
4.2.8 Status	40
4.3 Zone Settings	41
4.3.1 Zone Settings	41
4.3.2 Zone Event Settings	42
4.3.3 Alarm Pop-up Window Settings	43
4.4 Broadcast Settings	44

Chapter 1 Overview

1.1 Description

DS-PEA series of active panic alarm station supports multiple networks. It provides live view, two-way audio, and customized audio input. It supports linkage with the surrounding cameras and external lamp, sound box, etc. It helps to realize alarm aid in emergency.

1.2 Key Features

- Network adaptive and video and audio adaptive
- Audio and video file storage
- H.264/H.265, G.711U, G726
- Video collection and all-day monitoring with 2MP HD IR camera
- Built-in omnidirectional microphone to realize two-way audio
- Multiple network protocols including TCP/IP, SNMP, RTSP and SADP
- Supports Hik-SIP, Ehome, and Ezviz
- Waterproof, anti-electromagnetic interference, tamper-proof, explosion-proof, and anti-lightning (Panic Alarm Station doesn't support waterproof)

Chapter 2 Structure Description



2.1 Mainboard Description

2.2 Appearance Description

2.2.1 Panic Alarm Station



Figure 2-2 One-touch Panic Alarm Station

No.	Description
1	Loudspeaker
2	IR Light
3	Camera
4	Light Sensor
5	Panic Alarm Button
6	Microphone

Table 2-1 Panel Description

2.2.2 Box Panic Alarm Station



Figure 2-3 Case Panic Alarm Station

_		Table 2-2 Panel Description
	No.	Description
	1	Audible Alarm Lamp
	2	Loudspeaker
	3	IR Light
	4	Camera
	5	Light Sensor
	6	Panic Alarm Button
	7	Microphone

2.2.3 Pole Panic Alarm Station



No.	Description
1	Audible Alarm Lamp
2	Microphone
3	IR Light
4	Camera
5	Light Sensor
6	Loudspeaker
7	Panic Alarm Button

Figure 2-4 Pole Panic Alarm Station

2.3 Installation and Connections



- The product is suitable for mounting on concrete or other non-combustible surface only.
- For PLUGGABLE EQUIPMENT, the socket-outlet shall be installed near the equipment and should be easily accessible.
- For PERMANENTLY CONNECTED EQUIPMENT, a readily accessible disconnect device (2.5A) shall be incorporated external to the equipment.

2.3.1 Power Supply Wiring





2.3.2 Network Wiring



Figure 2-6 Network Wiring

2.3.3 Audible and Visual Alarm Wiring



Figure 2-7 Audible and Visual Alarm Wiring

2.3.4 Alarm Input Wiring (Normally Open)



Figure 2-8 Alarm Input Wiring (Normally Open)

2.3.5 Pole Panic Alarm Station Installation

Pole Panic Alarm Station (without Speed Dome Bracket)Dimension



Figure 2-9 Pole Panic Alarm Station (without Speed Dome Bracket)Dimension

Pole Panic Alarm Station (with Speed Dome Bracket)Dimension



Figure 2-10 Pole Panic Alarm Station (with Speed Dome Bracket)Dimension



Pole Panic Alarm Station Grounding Cage Dimension(without Speed Dome Bracket)

Figure 2-12 Pole Panic Alarm Station Grounding Cage Dimension(without Speed Dome Bracket)

Pole Panic Alarm Station Grounding Cage Dimension(with Speed Dome Bracket)



Figure 2-13 Pole Panic Alarm Station Grounding Cage Dimension(with Speed Dome Bracket)

Chapter 3 Activating the Control Panel

Purpose:

You are required to activate the control panel first before you can use the control panel. Activation via SADP, and Activation via client software are supported.

Activation via SADP Software

SADP software is used for detecting the online device, activating the device, and resetting the password.

Get the SADP software from the supplied disk or the official website, and install the SADP according to the prompts. Follow the steps to activate the control panel.

Steps:

- 1. Run the SADP software to search the online devices.
- 2. Check the device status from the device list, and select an inactive device.

ID	 Device Type 	Security	IPv4 Address	Port	Software Version	· · · ·	· ·	Device Serial No.	
001	DS-KD8402-VM	Active	10.16.6.85	8000	V1.4.0build 1606	10.16.6.254	80	DS-KD8402-VM012(
002	DS-KM8301	Active	10.16.6.96	8000	V1.3.2build 1602	10.16.6.254	80	DS-KM8301012016(_
	DS-KM8301	Active	192.0.0.64	8000	V1.4.0build 1608	192.0.0.		DS-KM830101201	
004	UNKOWN-DEVICE-TYPE	Active	10.16.6.126	8000	V5.4.0build 1602	10.16.6.254	80	20141119CCWR49	The device is not activated
005	DS-KD3002-2A	Active	10.16.6.127	8000	V1.3.2build 1602	10.16.6.254	80	DS-KD3002-2A0120	
006	DS-19A08-01BNG	Active	10.16.6.177	8000	V2.2.0build 1607	10.16.6.254	N/A	DS-19A08-01BNG20	
007	DS-PEA01-B	Active	10.16.6.92	8000	V1.0.1build 1607	10.16.6.254	N/A	DS-PEA01-B012016(
008	DS-K1T803MF	Active	10.16.6.111	8000	V1.0.0build 1608	10.16.6.254	80	DS-K1T803MF20160	You can modify the network parameters aft
009	DS-K2604-G	Active	10.16.6.222	8000	V1.1.1build 1602	10.16.6.254	N/A	DS-K2604-G201602:	the device activation.
									Activate Now
									New Password:
									Strong
									Confirm Password:

3. Create a password and input the password in the password field, and confirm the password.

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 **OK** to save the password.

You can check whether the activation is completed on the popup window. If activation failed, please make sure that the password meets the requirement and then try again.

5. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.

Modify Network	Parameters
Enable DHCP	
Device Serial No.:	DS-19A08-01BNG20151223V0201
IP Address:	10.16.6.202
Port:	8000
Subnet Mask:	255.255.255.0
Gateway:	10.16.6.254
IPv6 Address:	
IPv6 Gateway:	
IPv6 Prefix Length:	0
HTTP Port:	0
	ecurity Verification
Admin Password:	
	Modify
	Forgot Password

6. Input the password and click the **Modify** button to activate your IP address modification.

Activation via Client Software

The client software is versatile video management software for multiple kinds of devices.

Get the client software from the supplied disk or the official website, and install the software according to the prompts. Follow the steps to activate the control panel.

Steps:

1. Run the client software and the control panel of the software pops up, as shown in the figure below.



- 2. Click the **Device Management** icon to enter the Device Management interface, as shown in the figure below.
- 3. Click Add Device Type to enter the adding device type page.
- 4. Select Security Control Panel.

File System View Tool Help	💩 iVMS-4200	anna 🤁 🕮 🛗 13:47:35 🔒 🗕 🗗 🗙
📰 Control Panel 💆 Device	Management	
🗱 Server 📹 Group		
Organization	Device for Management (1)	
Encoding Device/Door Station	🕂 Add Device 🖸 Modify 🗱 Remove 🌵 Remote Configuration 🌻 Activation 😌 Refresh All	Filter
Security Control Panel	Nickname IP Device Serial No. Security Net Status Refresh	
💠 Add New Device Type	v Add New Device Type × ng 📀 📀	
	Select Device Type for the Client	
	Device Type:	
	Encoding Device/Door Station Storage Server	
	Stream Media Server Decoding Device	
	Cascading Server Transcoder	
	Hik Cloud P2P Device Security Control Panel Indoor Station/Master Station	
	C Device Type Instruction *	*
	OK Cancel	Filter
	I Device type Intrinvare version Security Server Port Start Time Added	
🙆 👃 🖾 🔹		* = *

- 5. Click Security Control Panel in the Organization list.
- 6. Check the device status from the device list, and select an inactive device.
- 7. Click the **Activate** button to pop up the Activation interface.
- 8. Create a password and input the password in the password field, and confirm the password.

	Activation		×
User Name:	admin		
Password:	•••••		
	Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.	Strong	
Confirm Password:	•••••		
	ОК	Cancel	

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.

- 9. Click **OK** button to start activation.
- 10. Click the **Modify Netinfo** button to pop up the Network Parameter Modification interface, as shown in the figure below.

Panic Alarm Station• User Manual

	Modify Network Parameter	×
Device Information:		
MAC Address:	44-19-b6-c0-af-a8	Сору
Software Version:	V1.2.1build 160919	Сору
Device Serial No.:	DS-KD8002-2A0120150515RR518919529	Сору
Network Information:		
Port:	8000	
Save IPv4 Settings		
IP Address:	10.16.6.144	
Subnet Mask:	255.255.255.0	
Gateway:	10.16.6.254	
Save IPv6 Settings		
Password:		
	ОК	Cancel

- 11. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.
- 12. Input the password to activate your IP address modification.

Chapter 4 Device Remote Operation

For properly running the system, set a login password to activate the panic alarm station before the first use. You can activate the device via SADP or client software. The factory settings are show as follows.

IP address: 192.0.0.65

Port No.: 8000

Admin User NameP: admin

4.1 Device Management

Purpose:

In this section, you are able to configure or view the basic parameters (such as the system information, alarm information, network data, device status and so on) of the device.

4.1.1 Add a Device

Steps:

- 1. Click the icon on the control panel to enter the Device Management interface and click the Server tab.
- 2. Click Add New Device Type on the Organization list and select Security Control Panel.
- 3. Click **OK** to save the settings, and the added security control panel type is displayed on the Organization list.

File System View Tool Help				🤷 iN	/MS-4200				anna 🤁 🗱 🛗 13:47:35 🔒 🗕 1	a ×
Control Panel 🛃 Device	Management									
🖬 Server 🗃 Group										
Organization	Device for Manage	ement (1)								
Encoding Device/Door Station	+ Add Device	🖾 Modify	X Remove	Remote Configuration	n 🌻 Activation	Refresh All			Filter	
Security Control Panel	Nickname	IP	Device Se	rial No.		Security	Net Status	Refresh		
+ Add New Device Type	v		Add	New Device Type		× ng	0	Ð		
	Select Device	Type for the C	lient							
	Device Type:									
		g Device/Door	Station	Storage Server						
		ledia Server		Decoding Device						
	Cascadi	ng Server d P2P Device		 Transcoder Security Control F 						
	_	d P2P Device tation/Master S	tation	 Security Control F 	anei					
	c Device Type In:	struction				*				
						Cancel			Filter	
	1	Device Type		innware version	security	server Fort Start Tir	me	Added		
🙆 🕭 🗃 🔹									× =	

- 4. Click Security Control Panel and click Add Device to add the device to the management list of the software.
- 5. You can add the active online devices in the same local subnet with the client software, or select the adding mode by IP/Domain Name, by IP segment, by IP Server, or by HiDDNS, and configure the corresponding settings for the device. Take **IP/Domain Name** as an example.

	Add		×
Adding Mode: IP / Domain Name IP Se	gment	IP Server	
Nickname: Address:			
Port:	8000		
User Name:	admin		
Password:	•••••	•	
 Export to Group 			
Set the device name a connected to the devi		ne and add all the channels	
		Add	Cancel

- Input the required information.
 Nickname: Edit a name for the device as you want.
 Address: Input the device's IP address or domain name.
 Port: Input the device port number. The default value is 8000.
 User Name: Input the device user name.
 Password: Input the device password.
- 7. Optionally, you can check the checkbox **Export to Group** to create a group by the device name. All channels and alarm inputs of the device will be imported to the corresponding group by default.
- 8. Click **Add** to add the device.

4.1.2 Edit a Device

Purpose:

You can edit the device information in this section, including the device name, address and port number. *Steps:*

- 1. On the **Device Management** interface, click and select a control panel in the device list.
- 2. Click on the **Modify** button on the upper side of the list to enter the device modify interface.

		Modify		×
Adding Mode: IP / Domain Name	e 🕓 IP Segment	IP Server		
Nickn	name:	xxxxxxxxxxxxx		
Addre	ess: 10.	14.2.252		
Port:	80	00		
User	Name: adi	min		
Pass	word:	•••••		
			Modify	Cancel

- 3. Enter the required nick name, address, and port number and then enter the admin username and password.
- 4. Click **Modify** to save the changes.

4.1.3 Delete a Device

Select device from the list, click **Delete**, and then you can delete the information of the selected device.

4.1.4 Status

🖭 🚳 System Partition System Status 🖭 🚳 Network Partition System | Status of Guard 🖭 🚳 Storage Partition Syste... Away Arming 🖭 🍪 Alarm Partition Syste... Disabled 🖭 🚳 Other Partition Syste... Disabled 🗄 🚳 Image Partition Syste... Disabled 🖭 🚳 Event Partition Syste... Disabled 🕑 🍪 Operation Partition Syste... Disabled – 💰 Status Partition Syste... Disabled 🔅 Par Partition Syste... Disabled Zone 🎡 Trigge 🎡 Siren 🎡 Storage Battery Refres

Click Remote Configuration > Status to view status of the partition, zone, trigger, siren ,and storage battery.

4.2 Remote Configurations

Purpose:

In this section, you are able to configure device parameters remotely. Click the **Remote Configuration** button to enter the interface.

🔅 Device Information	Basic Information					
🎡 General	Device Type:	DS-PEA20-P/AIO	Local RS-485 Number:	0		
🎡 Time	Local Zone Number:	3	Extended RS-485 Number::	0		
System Maintenance	Extended Zone Number:	0	Sub-system Number:	0		
log	Local Trigger Number:	1	Public Sub-system Num	0		
🎡 User	Extended Trigger Number:	0	Keyboard Number:	0		
Security	Local Sensor Number:	0	Global Keyboard Number:	0		
Password Management Network	Extended Sensor Number:	0	Analog Camera Number:	1		
General	Siren Number:	1	Network User Number:	1		
Wetwork Center Configuration	Electric Lock Number:	1	Mobile Gate Number:	0		
Call Center Configuration	Alarm Lamp Number:	1				
Advanced Settings	Device Serial No.:	INo.: DS-PEA20-P/AIO0120170912AAWR662688720CV				
🎡 CMS	Version Information					
🎡 Sip Config	Firmware Version:	V1.1.1 build 170808				
🎡 Configuring the Hik Cloud P2	Hardware Version:	0x601				
🚯 Storage						
🗟 🚳 Alarm						
🚯 Other						
🚳 Image						
🕼 🕼 Event						
🚳 Operation						
🕼 Status						

4.2.1 System Information Settings

Purpose:

In this section, you can configure the system parameters (such as time, log, user, security, system maintenance and so on) for the device.

	Re	emote Configuration		
- 🗞 System	Displaying the Device	e Information		
🏶 Device Information	Basic Information			
🎡 General	Device Type:	DS-PEA20-P/AIO	Local RS-485 Number:	0
🎡 Time	Local Zone Number:	3	Extended RS-485 Number::	0
System Maintenance	Extended Zone Number:	0	Sub-system Number:	0
🎡 Log	Local Trigger Number:	1	Public Sub-system Num	0
🎡 User	Extended Trigger Number:	0	Keyboard Number:	
🎡 Security	Local Sensor Number:		Global Keyboard Number:	
🎡 Password Management	Extended Sensor Number:		Analog Camera Number:	
– 🚳 Network	Siren Number:		Network User Number:	
🎡 General				
Wetwork Center Configuration	Electric Lock Number:		Mobile Gate Number:	0
🎡 Call Center Configuration	Alarm Lamp Number:			
Advanced Settings	Device Serial No.: DS-PEA20-P/AI00120170912AAWR662688720CV			
🎡 CMS	Version Information			
🎡 Sip Config	Firmware Version:	V1.1.1 build 170808		
🎡 Configuring the Hik Cloud P2	Hardware Version:	0x601		
🗉 🚳 Storage				
🗄 🚳 Alarm				
🗄 🚯 Other				
t 🗞 Image				
1 🚯 Event				
🗄 🚷 Operation				
t 🚯 Status				

General Settings

Steps:

1. Click Remote Configuration > System > General to enter the general parameters configuration interface.

System	Configuring the Gener			
Device Information	Device Information			
🏶 General	Device Name:	Embedded Net EA		
🎡 Time	Device No.:			
🎡 System Maintenance				
🎡 Log	Overwrite Record Files:			
🎡 User		Save		
Security				
Password Management				
🗆 🚳 Network				
🎡 General				
Wetwork Center Configuration				
🎡 Call Center Configuration				
Advanced Settings				
🎡 CMS				
🎡 Sip Config				
② Configuring the Hik Cloud P2				
🛨 🚳 Storage				
🗄 🚳 Alarm				
🗄 🚳 Other				
🛨 🚳 Image				
🖭 🍪 Event				
🗉 🚳 Operation				
🐮 🍪 Status				

- 2. Input the device name and device number.
- 3. Click the drop down menu to select whether to overwrite the record files.
- 4. Click **Save** to save the settings.

Timing Settings

Purpose:

Before you start configuring the security control panel, you need to do timing for the device first.

Steps:

1. Click **Remote Configuration > System > Time** to enter the time configuration interface.

	Re	mote Configuratio	n		×
- 🗞 System	Configuring the Time Time Zone	Settings (e.g.	, NTP, D	ST)	
 General Time Concernation 	Select Time Zone:	(GMT+08:00) Beij	ing, Hong H	Kong, Perth, Singa 🔻	
 System Maintenance Log User Security Password Management 	Server Address: NTP Port Sync Interval:	123		Minute(s)	
C Network C Network C Storage C Alarm C Other C Intage	Enable DST Start Time: End Time: DST Blas:	October 🗸 L	First Week .ast Week	 ✓ Sun ✓ 2 ✓ Sun ✓ 2 ✓ Sun ✓ 2 	
 C Event C Operation C Status 	Synchronization				Save

2. Click Synchronization to do timing.

System Maintenance

The device supports system maintenance remotely. Click **Remote Configuration > System > System Maintenance** to enter the interface.

l		Rem	ote Configuration		,
	🖃 🚳 System	System Maintenance			
	Device Information	System Management			
	🎡 General		Reboot		
	🎡 Time		Restore Default Settings		
	🌸 System Maintenance		Restore All		
	🎡 Log		Import Configuration File		
	🎡 User		Export Configuration File		
	Security	Remote Upgrade	Export Conliguration The		
	🎡 Password Management				
	🐮 🚳 Network	Security Control Pan ~		··· Upgrade	
	🕐 🚳 Storage	Progress:			
	🐮 🚳 Alarm				
	🛃 🚳 Other				
	🐮 🚳 Image				
	🕐 🚳 Event				
	💿 🚳 Operation				
	🕐 🚳 Status				
1					

- Restart the System
- Click Reboot to restart the device.
 - Restore Default Settings

Click **Restore Default Settings** to restore the default settings.

	~1	D	_
N	0	Т	Е

Except the IP address and user parameters, all other parameters of the device will be restored to factory default settings.

Restore All the Parameters to Default

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



After restoring the parameters to default, the device needs to be restarted.

- Import Configuration File
- The device supports importing the configuration file. Click Import Configuration File to import the file.
- Export Configuration File
- The device supports exporting the configuration file. Click **Export Configuration File** to export the file.
- Import/Export IPC Configuration File

The device supports importing/exporting the IPC configuration file. Click **Import/Export IPC Configuration File** to import/export the file.

Remote Upgrade

The device also supports remote upgrading. You can select the upgrade file including security control panel upgrading file and alarm keypad upgrading file. Click is select the local upgrading file and click **Upgrade** to upgrade the device. The upgrading progress is shown below.

You need to enter the keypad address for keypad remote upgrade.



After upgrading, the device needs to be restarted.

Log Searching

Click **Remote Configuration > System > Log** to search and view the logs. Set the search mode, major type, minor type, start time and end time, and then click **Search** to search the log.

	_	Remote	Configuration	_		×
 System Device Information General Time System Maintenance Log User Security Password Management Sorage Storage Storage Sorage 	Searching Search Mode: Major Type: Start Time: Index	Remote and Viewing th All All 2017-09-12 00: Operation Time	e Logs	Minor Type: End Time: Minor Type	All Control of the search Remote O Local Oper Remote H	
 	4				Backup	•

User Settings

Purpose:

You can add, edit, or delete the user in this section.

- Add an admin User (Only one admin user can be added)
- Steps:
- 1. Click Remote Configuration > System > User to enter the user configuration interface.

🎡 General	🕄 Add	📝 Edit	T Delete	
🎡 Time	User Name	Priority	IP Address	MAC Address Password Security
🎡 System Maintenance	admin	Administrator	0.0.00	00:00:00:00:00 Strong
🔮 Log				
🏶 User				
Security				
Password Management				
🖭 🚳 Network				
🕐 🚳 Storage				
🕐 🚳 Alarm				
🕐 🍪 Other				
🖈 🚳 Image				
🖭 🚳 Event				
🖈 🌀 Operation				
🖭 🚳 Status				
	•			

Jser Information				
Jser Type:	Administrator	 User Na 	me:	admin
assword:	•••••	Confirm	Password:	•••••
Address:	0.0.0.0	MAC Add	Iress:	00:00:00:00:00:00
Iser Primission				
 Remote Paramete Get Parameters Restore Default S Remote Upgrade Trigger Control Remote Voice Tal 	ettings			

- 3. Enter the corresponding user information including the user type, user name, password, IP address, and MAC address.
- 4. Select the permission of the user.
- 5. Click **OK** to finish the settings.

Edit a User

Steps:

1.

Click	☑ Edit t	o enter the interface of editing the selected user.
		User Parameter

User Information			
User Type:	Administrator	 User Name: 	admin
Password:	•••••	Confirm Password:	•••••
IP Address:	0.0.0	MAC Address:	00:00:00:00:00:00
User Primission			
 Remote Opera Arm Remote Log S Remote Shutd Remote Param Get Parameter Restore Defau c' 	own / Reboot neter Settings 's		

- 2. Edit the corresponding user information including the user type, user name, password, IP address, and MAC address.
- 3. Edit the permission of the user.
- 4. Click **OK** to finish the settings.
- Delete a User

Steps:

- 1. Select a user needs to be deleted.
- 2. Click Delete to delete the user.

Password Management

Click Remote Configuration > System > Password Management to set the maximum password attempts and lock duration.

	Re	mote Configuration			
= 🚳 System	Configuring the Pass	word Management			
 Device Information General Time System Maintenance Log 	Max. Password Attempts: Lock For: IP Address		S		
 Wser Security Password Management 					
🗈 🕜 Status					
				Save	Unlock All

4.2.2 Network Settings

Purpose:

You can edit the general network parameters in this section.

General Network Parameters Settings

Steps:

1. Click **Remote Configuration > Network > General** to enter the general network configuration interface.

🛾 🚷 System	Configuring the Networ	K Farameters	
② Device Information	Mode A:	Multi-address ~	
🎡 General			
🎡 Time	NIC1:		
🎡 System Maintenance	NIC Type:	10M/100M/1000M Self ~	
🎡 Log		Auto-obtain	
🎡 User	IPv4 Address:		
Security	Subnet Mask (IPv4):		
🎡 Password Management	Default Gateway (IPv4):		
🚳 Network		00:40:57:bf:8e:a0	
🏶 General	MTU(Byte):		
Wetwork Center Configuration	Device Port:		
Call Center Configuration	Default Route:	NIC 1	
Advanced Settings	RTSP Port	554	
CMS			Sav
 Sip Config 			Sav
Sip Configuring the Hik Cloud P2			
Storage			
🗟 Alarm			
🚳 Other			
🚳 Image			
🚳 Event			
🚳 Operation			
🕼 Status			

- 2. Configure the NIC setting.
- 3. Click **Save** to save the above settings.

Network Center Settings

Purpose:

In this section, you can configure the parameters (such as server type, IP address, port NO., and so on) of the network center. *Steps:*

1. Click Remote Configuration > Network > Network Center Configuration to enter the network center configuration interface.

	Ren	note Configuration		
🖈 🔞 System	Configuring the Netwo	ork Center Parame	ers	
- 🚯 Network	NIC1:	NICI	~	
🎡 General	NICT.	Enable Upload Cer		
🛞 Network Center Configuration	Notify Surveillance Center:		~	
🎡 Call Center Configuration	Server Type:	IP4/IP6	~	
Advanced Settings	IP Address:	0.0.0.0		
🎡 CMS		7200		
🎡 Sip Config	Protocol Type:		~	
Configuring the Hik Cloud P2	User Name:			
🕐 🚳 Storage		Save		
🛨 🍪 Alarm				
🐮 🚳 Other				
🛧 🚳 Image				
🐮 🚳 Event				
🛨 🚳 Operation				
衝 🍪 Status				

- 2. Click and select a network center. Two centers are selectable.
- 3. Click Enable Upload Center.
- 4. Click the dropdown menu to select a sever type. Two sever types are available: IP4/IP6 and domain.
- 5. Enter the IP address which is used to communicate with the network alarm receiving center.
- 6. Enter the port NO. for communicating with the alarm receiving center.
- 7. Click the dropdown menu to select the protocol type.
- 8. Enter the username which is applying for displaying in the alarm receiving center.

NOTE

The length of the username should be 6 characters. Only numeric (0~9), and letter (A~F&a~f) are valid for this username.

Call Center Settings

Purpose:

You can configure the parameters (such as report uploading time period, center name, phone number and so on) for each call center in this section.

Steps:

1. Click **Remote Configuration > Network > Call Center Configuration** to enter the call center configuration interface.

Panic Alarm Station• User Manual

😪 🗞 System	Configuring the Call	Center Parameters	
🐼 Network	Center Parameters		
🎡 General	Center Type:	Center1 ~	
🎡 Network Center Configuration	Center Name:	Center1	
🔅 Call Center Configuration	Center Phone Number:		
Advanced Settings	Dialing Times:	5	
CMS	Communication Protocol:	CID ~	
🎡 Sip Config	Transfer Mode:	DTMF 5/S	
② Configuring the Hik Cloud P2	Receiver ID:		
🗞 Storage			
🛾 🚳 Alarm			Save
🚯 Other			
🕜 🕼 Image			
🕼 Event			
🕜 🚳 Operation			
🕼 Status			

- 2. Select a center type (only center 1 is available).
- 3. Enter the center name and phone number. 0

NOTE

- The maximum length of center name is 32 characters. •
- The phone number should be 31 characters and the input mode is
- {NO.}{Dwell Time}{EXT NO.}. For example, in the number of 000088075998FFF8180, the letter F (which means 2 seconds) represents the dwell time, if the number of the letter F is N, the dwell time is N*F seconds. The number of F is suggested to be more than 3, which means the dwell time should be more than 6 seconds.
- Enter the dialing times (1~15). The dialing times represents the times that the control panel trying to communicate the alarm 4. receiving center.
- 5. Select the communication protocol.
- 6. Select the transmission mode: DTMF5/S and DTMF10/S.
- 7. Enter the receiver ID which is the authentication account while doing the communication with the alarm receiving center.
- 8. Click Save to save the settings.

Advanced Network Parameters Settings

Steps:

1. Click Remote Configuration > Network > Advanced Settings to enter the advanced network configuration interface.

	Rem	note Configuration	
- 🗞 System	Configuring the Advan	ced Network Settings	
 Device Information General Time System Maintenance Log User Security 	DNS1 IP Address: DNS2 IP Address: Alarm Host IP: Alarm Host Port	0.0.0.0	
 Password Management Content Network General Network Center Configuration Call Center Configuration 			
 Advanced Settings CMS Sip Config Configuring the Hik Cloud P2 			
🕈 🌚 Status			

- 2. Enter the corresponding DNS sever address.
- 3. Enter the IP address and port NO. of the control panel.
- 4. Click **Save** to save the settings.

CMS Settings

Purpose:

CMS is used to configure EHome protocol parameters for the device.

Steps:

1. Click **Remote Configuration > Network > CMS** to enter the CMS configuration interface.

	Rem	ote Configuration	
– 🐼 System	Configuring the CMS F	arameters	
🎡 Device Information	ID:	1	~
🎡 General	Server Type:		• •
🎡 Time			-
🎡 System Maintenance	IPv4 Address:		
🎡 Log	IPv6 Address:		
🎡 User		7660	
🎡 Security	Communication Network:		~
Password Management	Protocol Type:		×
= 🗞 Network	Device Status:	Offline	~
🎡 General	Device ID:	000000	
Wetwork Center Configuration		Save	
🎡 Call Center Configuration			
Advanced Settings			
🍪 CMS			
🎡 Sip Config			
Configuring the Hik Cloud P2			
衝 🚳 Storage			
🕙 🚳 Alarm			
🐮 🚳 Other			
🐮 🚯 Image			
🐮 🚯 Event			
🐮 🚳 Operation			
🐮 🚯 Status			

- 2. Click the dropdown menu to select a sever type. Two sever types are available: IP4/IP6 and domain.
- 3. Enter the IP address which is used to communicate with the service.
- 4. Enter the port NO. for communicating with the service. The default port NO. for EHome protocol is *7660* and for privacy protocol is *10001*.
- 5. Click the dropdown menu to select the communication network. Four types are available: Auto, Wired Network Priority, Wired Network and Wireless Network.
- 6. Enter the device ID where the CID report comes from.

NOTE

- The length of the device ID should be 6 characters.
- Only numeric (0~9), and letter (A ~ F & a ~ f) are valid for this device ID.
- 7. Click **Save** to save the settings.

Sip Settings

Steps:

1. Click Remote Configuration > Network >Sip Config to enter the Sip configuration interface.

Panic Alarm Station• User Manual

	_	Remote Configu	ration	_	_	_
衝 🚳 System	Configure Sip	parameters				
🖃 🚳 Network	Enable					
Network Center Configuration Call Center Configuration	Login Status: Ip Addr:	Logined				
Advanced Settings	Server Port: Local No.:					
 CMS Sip Config 	Display Name:	22222				
 [™] Configuring the Hik Cloud P2 [™] [™]	Login Cycle:	10	Mir	ute(s) ve		
* 🗞 Alarm						
🕙 🚳 Operation						
🕐 🗞 Status						

- 2. Check **Enable** box to enbale the Sip server.
- 3. Enter the Sip server parameters including IP address, port No., local No., display name, login cycle.

2	1
101	ΓE

- The server port No. ranges from 1024 to 65535.
- The device ID ranges from 0 to 999999.
- The characters of local No. should be 1 to 64.
- The login cycle ranges from 1 to 30 (min)
- 4. Click **Save** to save the settings.

4.2.3 Storage

HDD Information `

Steps:

1. Click **Remote Configuration > Storage > General** to enter the HDD Settings interface. You can view the capacity, free space, status, type and property of the disk.

	Remote Configuration ×
🐮 🚳 System	Configuring the HDD Parameters
🗄 🚳 Network	HDD No. Capacity(GB) Free Space(GB) Status
– 🚷 Storage	
🌸 General	
🎡 File	
🗄 🚳 Alarm	
🗄 🚳 Other	
🗉 🚳 Image	
🗉 🚳 Event	Modify Format Update
🗉 🚳 Operation	
🗄 🚳 Status	Progress: D%
	Entrational Contraction of the second s

- 2. If the status of the HDD is **Uninitialized**, check the corresponding checkbox to select the disk and click Format to start initializing the disk. When the initialization completed, the status of disk will become **Normal**.
- 3. Click **Save** to save the settings.

NOTE

This function is available only if the device is connected with HDD.

File Query

Steps:

1. Click Remote Configuration > Storage > File to enter the file query interface.
| | | Remote Config | uration | | | |
|-----------------------------|------------------------|---------------------|----------|------------------------------|----------|-----------|
| 🛨 🍪 System | Searching | and Viewing the Red | ord File | s | | |
| * 🗞 Network
– 🗞 Storage | Camera:
Start Time: | Camera01 | | Recording Type:
End Time: | CMR ~ | Q. Search |
| 🎡 General | 🗆 Index File | | Size | Start Time | End Time | |
| ± ⓒ Alarm
± ⓒ Other | | | | | | |
| • 🗞 Image
• 🗞 Event | | | | | | |
| • 🗞 Operation
• 🗞 Status | | | | | | |
| 🛨 🌚 Status | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | Download |

- 2. Enter the search criteria including camera name, property, start time and end time.
- 3. Click **Search** to get the file list.

4.2.4 Alarm Settings

Zone Settings

Steps:

1. Click **Remote Configuration > Alarm > Zone** to enter the Zone configuration interface.



2. In the Alarm Input list, select an alarm input channel and click the icon 🖉 to enter the zone setting interface.

Zone Settings	×
Zone No.:	1
Name:	Alarm In
Detector Type:	Emergency Switch 🗸
Zone Type:	Shield Zone 🗸
Sensitivity:	500ms 🗸
Audio File:	
	Upload Alarm Recover
Linked Alarm Lamp	Li Linked Tr Other
Select All	I
Siren 1	
Сору То	Save Cancel

- Edit the general information of the Zone, including name, detector type, zone type, sensitivity and so on.
 Detector Type: Select the type of the detector.
 Zone Type: Select the type of Zone in the partition.
 Sensitivity: Select the response time of the Zone.
- 4. Select the linked siren and linked trigger.
- 5. Click **Copy to** to copy all these settings to other Zones.
- 6. Click **Save** to save the settings.

Trigger Settings

Steps:

1. Click **Remote Configuration > Alarm > Trigger** to enter the trigger configuration interface.

		Remote Configuration		
🐮 🇞 System	Configuring the T	rigger Parameters		
🖭 🚳 Network	Trigger Name	Output Delay(s)		Settings
• 🗞 Storage – 🗞 Alarm	1 AlarmOut_1	0		Ø
@ Zone				
🔅 Trigger	1	🛃 Trigger Parameters Setting	gs 📃 🗙	
Waiting		Trigger:	1	
Alarm Lamp Flicking Voice Prompt			AlarmOut_1	
🎡 Audio File				
• 🗞 Other • 🗞 Image		Copy to	Save Cancel	
🐮 🍪 Event				
衝 🚳 Operation				
🐮 🚱 Status				

2. In the Alarm Output list, select the alarm output channel and click the icon 🖉 to enter trigger parameters setting interface.

Irigger Parameters Setti	ngs	23
Trigger:	1	
Name:	AlarmOut_1	
Output Delay(s):	0	
Copy to	Save Cancel	

- Edit the general information of the trigger, including name, output delay and so on.
 Output Delay (0~5999s): Configure the alarm output time after the alarm being triggered.
- 4. Click **Copy to** to copy all these settings to other Zones.
- 5. Click **Save** to save the settings.

Calling Waiting Settings

Steps:

1. Click Remote Configuration > Alarm > Waiting to enter the trigger configuration interface.

		Remote Configuratio	'n	
🗄 🔞 System	Configuring Call	Waiting Settings.		
 ♥ System ♥ Network ♥ Storage ♥ Alarm ♥ Zone ♥ Trigger ♥ Waiting ♥ Alarm Lamp Flicking ♥ Voice Prompt ♥ Audio File ♥ Other 	Max. Ring Duration: Waiting Time:	60	Save	\$ \$
 c Image c Event c Operation b c Status 				

- 2. Enter the Max. ring duration (40s to 80s) for reporting alarm to the center.
- 3. Enter the waiting time (10s to 60s) for the center to answer the call.
- 4. Click Save to save the settings.

Alarm Lamp Settings

Steps:

1. Click Remote Configuration > Alarm > Alarm Lamp Flicking to enter the trigger configuration interface.

	Remote Configuration	×
🐮 🍪 System	Configuring Alarm Lamp Flicking Settings.	
 	Alarm Lamp Flicking Lamp Schedule	
는 🗞 Alarm ŵ Zone ŵ Trigger	Enable Alarm Lamp Flicking Duration(s): 180 Time Interval(s): 3600	
 Waiting Alarm Lamp Flicking Voice Prompt 		
 		
 ★ Content ★ Content 		
🕐 🗞 Status		
	Save	

- 2. Check Enable Alarm Lamp Flicking box.
- 3. Enter the alarm lamp flashing duration (s).
- 4. Enter the time interval for each flashing(s).
- 5. Click Save to save the settings.



If the duration is 180s and the time interval is 3600s, the alarm lamp flashes 3 minutes each hour.

Voice Prompt Settings

Steps:

1. Click Remote Configuration > Alarm > Voice Promptto enter the trigger configuration interface.

- 2. Check Enable Alarm Lamp Flicking box.
- 3. Select Female/Male voice for center busy file, refuse, and voice talking prompt.
- 4. Select the ring tone.
- 5. Slick **Save** to save the settings.

4.2.5 Image Settings

Video& Audio Settings

Steps:

1. Click Remote Configuration > Image > Video & Audio to enter the video/audio configuration interface.

🛛 🚳 Network	Camera:	Camera1		~		
🗞 Storage	Video	Gamera				
🚯 Alarm						
🗟 🚳 Other	Stream Type:	Main Stream	~	Video Type:	Video & Audio	~
Partol Card	Bitrate Type:	Constant	~	Bitrate:	2048 Kbps 🗸	
Martol Card	Video Quality:	Medium	~	Resolution:	HD720P(1280*720)	~
	Frame Rate:	Full Frame	~	I Frame Interval:	25	÷
🔅 Video & Audio	Audio Encoding Type:			Video Encoding Type:		~
Wideo Display		_	~	video Encoding Type.	STD_H264	v
Image Settings	File Size Per Day: Audio	21.0G				
🎡 Intercom Audio	Audio					
🕼 Event	Volume:		_			
🗟 🔞 Operation						
🕼 Status	Copy to					Sa
j eg otatas						

- 2. Select a camera needs to be configured.
- 3. Edit the general video parameters.

Scream Type: The main stream is usually for recording and live viewing with good bandwidth, and the sub-stream can be used for live viewing when the bandwidth is limited.

Video Type: Select the stream type to video stream, or video & audio composite stream.

Bitrate Type: Select the bitrate type to constant or variable.

Resolution: Select the resolution of the video output.

Frame Rate: The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

I Frame Interval: Set the I-Frame interval from 1 to 400.

4. Click **Copy to** to copy all these settings to other Zones.

5. Click Save to save the settings.

OSD Settings

Steps:

1. Click **Remote Configuration > Image > Video Display** to enter the OSD Settings interface.

	_	Remote Configuratio	n		×
🕑 🌚 System	Configuring	the Display Parameters	, including O	SD, Privacy Mask, etc.	
🖭 🚳 Network	Camera:	Camera1	~		
🕑 🌀 Storage				Display Camera Name	
🕑 🚳 Alarm – 🌚 Other				 Display Date 	
Partol Card				Display Week	
- 🗞 Image					
Wideo & Audio					
🏶 Video Display					
🎡 Image Settings					
🎡 Intercom Audio					
🕑 🚳 Event					
 Coperation 	Camera Name:	Camera 01			
J Status	Date Format	MM-DD-YYYY ~			
	Time Format	24-hour 🗸			
	OSD Attribute:	Non-Transparent & N 👻			
	Сору То				Save

- 2. Check the corresponding checkbox to select the display of camera name, date or week if required.
- 3. Edit the camera name in the text field of **Camera Name**.
- 4. Select from the drop-down list to set the time format, date format and display mode.
- 5. Check the checkbox in front of textbox to enable the on-screen display.
- 6. Input the characters in the textbox.
- 7. Use the mouse to click and drag the red text frame **I** in the live view window to adjust the text overlay position.
- 8. Click **Save** to save the settings.

Image Settings

Steps:

1. Click Remote Configuration > Image > Image Settings to enter the image settings interface.

🖭 🚳 Network	Camera:	Camera1 ~	
🖭 🚳 Storage			
🛃 🍪 Alarm			
🖃 🌀 Other			
🎡 Partol Card			
🖃 🚳 Image			
🎡 Video & Audio			
🎡 Video Display			
🏶 Image Settings			
🎡 Intercom Audio			
🖭 🚳 Event			
🖭 🚳 Operation			
🖭 🍘 Status	Mode A:	Standard 🗸	
	Brightness:		
	Contrast:		
	Saturation:		
	Hue:		
	Sharpness:		
	Default Value		

2. Drag the 🖳 to adjust the brightness, contrast, saturation of the image.

3. You can also click Default Value to restore the default values.

4.2.6 Event Settings

Schedule Settings

Click Remote Configuration > Events > Schedule to enter the record schedule configuration interface.

	Re	temote Configuration
🕑 🚳 System	Configuring the Reco	ording Schedule
🕑 🚳 Network	Camera:	Camera1 ~
🕐 🚳 Storage	Record	
🖃 🚳 Alarm		
🎡 Zone		✓ Local Recording
🎡 Trigger		
🎡 Waiting	Recording Schedule:	: Template01 V
🎡 Alarm Lamp Flicking		Advanced Settings
Woice Prompt	Сору То	Save
🎡 Audio File		
🕑 🚳 Other		
🕑 🚳 Image		
🖃 🚳 Event		
🏶 Schedule		
🕐 🚳 Operation		
🕐 🚳 Status		

Record Schedule Settings •

Steps:

- Select the camera needs to be configured. 1.
- Check the checkbox of Local Recording to enable the device local recording. You can also check ANR checkbox to enable the 2. device continuing recording even if the network is off.
- Select from the drop-down list to set the recording type including Main Stream and Sub Stream. 3.
- Click the Template01 4.

icon to set the record schedule.



- 5. Click Edit to enter the Templates Management interface. Select the template to be set and you can edit the template name. Set the time schedule for the selected template. 6.

When the cursor turns to *weight*, you can edit the schedule time bar.

When the cursor turns to 🔍, you can move the selected time bar you just edited.

When the cursor turns to 🖾, you can lengthen or shorten the selected time bar.

7. Optionally, you can select the schedule time bar,

And then click the icon \bigotimes to delete the selected time bar,

Or click the icon 🔟 to delete all the time bars,

Or click the icon \Box to copy the time bar settings to the other dates.

- 8. Click **Save** to save the template, or click cancel to exit the interface.
- 9. Click **Advanced Settings** button to set the pre-record time, post record time, video expired time, redundant record and audio recording.

Advanced Settings			X
Pre-record:	5 s	~	
Post-record:	5 s	~	
Keep Record Files For:	0		Day
Redundant Record:	No	~	
Record Audio:	Yes	~	
	Save	Car	ncel

- 10. Click Copy to to copy all these settings to other Zones.
- 11. Click **Save** to save the settings.
- Capture Schedule Settings
- 1. Check the checkbox of **Capture Settings** to enable the device local capturing.
- 2. Click the remplate01 icon to set the capture schedule. For details, refer to Steps 5, 6, 7 in Record Schedule Settings.
- 3. Click **Copy to** to copy all these settings to other Zones.
- 4. Click **Save** to save the settings.

4.2.7 Operation

You can configure the trigger, siren, alarm lamp, electric lock, and audio in/out in this section.

Click **Remote Configuration > Operation** to enter the interface.

Trigger: you can select to turn on/off the selected trigger.

Siren: you can enable/disable the specified siren.

Alarm Lamp: You can enable/disable the alarm lamp.

Electric Lock: You can enable/disable the electric lock.

Audio In/Out: You can adjust the input volume and output volume.

4.2.8 Status

Click **Remote Configuration > Status** to view status of the partition, zone, trigger, siren ,and storage battery.

	Remote Configuration	
🖲 🚳 System	Partition System Status	
🐮 🔞 Network	Partition System Status of Guard	
🐮 🚷 Storage	Partition Syste Away Arming	
🖭 🍪 Alarm	Partition Syste Disabled	
🗄 🚳 Other	Partition Syste Disabled	
🗄 🚳 Image	Partition Syste Disabled	
🗄 🚳 Event	Partition Syste Disabled	
e 🔇 Operation	Partition Syste Disabled	
🖃 🚳 Status	Partition Syste Disabled	
Partition System Zone	Partition Syste Disabled	
🎡 Zone		
Siren		
Storage Battery		
ge storage battery		
	Refresh	

4.3 Zone Settings

4.3.1 Zone Settings

Steps:

- 1. Click **Device Management > Security Control Panel > Remote Configuration > Alarm > Zone** to enter the Zone configuration interface.
- 2. In the Alarm Input list, select an alarm input channel and click the icon 🖉 to enter the zone settings interface.

Config	guring the Zone	Parameters		
Zone	Name	Zone Type	Detector Type	Settings
1	Alarm In	Shield Zone	Emergency Switch	Ø
2	Alarm In	Shield Zone	Emergency Switch	Ø
3	Emergency Ca.	Emergency H	Emergency Switch	Ø

Edit the general information of the zone, including name, detector type, zone type, sensitivity, audio file etc.
 Detector Type: Select the type of the detector.
 Zone Type: Select the type of zone in the partition.

Sensitivity: Select the response time of the zone.

Zone Settings	<u> </u>		
Zone No.:	1		
Name:	Alarm In		
Detector Type:	Emergency Switch 🗸		
Zone Type:	Shield Zone 🗸		
Sensitivity:	500ms 🗸		
Audio File:			
	Upload Alarm Recover		
Linked Alarm Lamp L	i Linked Tr Other		
Select All			
Siren 1			
Сору То	Save Cancel		

- 4. Select the linked siren, alarm lamp, linked trigger and others.
- 5. Click **Copy to** to copy all these settings to other zones.

Coj	ру То	
Zone 1 Copy To		
Select All		
Zone 2		
Zone 3		
	Save	Cancel

6. Click **Save** to save the settings.

INOTE	
Four zone types in the Zone	Parameters: Instant Zone, Fire Alarm Arming Zone, 24 Hour Non-voiced Zone and Shield
Zone.	
Instant Zone	Alarm is sent out without any delay once the detector is triggered.
Fire Alarm Arming Zone	When the 24-hour armed zone is triggered by fire alarm, sirens will send out resonant and special sound.
24 Hour Non-voiced Zone	When the 24-hour armed zone is triggered, it will send alarm reports to the surveillance center without any audible warning. The 24 hour silence alarm zone is not affected by manual or scheduled arming/disarming.
Shield Zone	The alarm will not be triggered.

Panic alarm station has three zones among which two are ordinary zones and one is emergency zone.

4.3.2 Zone Event Settings

Steps:

1. Click **Control Panel > Event Management > Zone Event** to enter the Zone Event configuration interface.

Zone				🖹 Copy to 🔛 Save
Search	Zone Name.			
Alarm In_10.7.165.210	Linked Trigger	Linked Siren	Trigger Camera	
Alarm In_10.7.165.210			Search	
			E AL	
			 10.7.165.210 Cameral_10.7.165.210 	
		Trigger Client		
		Audible Warni		
		Email Linkage		
		Alarm Trigger		
		Alarm on E-map		

- 2. Select the corresponding zone on the left and then tick necessary items.
- 3. (Optional) Click Copy to to tick the necessary items.

Select Parameters to Copy:			
 Zone Type 	Linked Trigger	Linked Siren	
Trigger Client Action	Linked Camera		
Copy to:			
Search			9
All			
🖃 🔲 📹 10.7.165.210			
🗆 👑 Alarm In_10.7.165	5.210		
🗌 👑 Alarm In_10.7.165	5.210		

4. Click Save to save the settings.

The Alarm In is emergent by default.

4.3.3 Alarm Pop-up Window Settings

Purpose

When the devices are armed, the alarm intercom will pop up once the detectors are triggered.

Enable Pop-up Window Function

When the devices are arming, enable the pop-up window by following the steps bellow.

Steps:

1. Click **Tool > Device Arming Control** to enter the device arming control interface.

🖴 Device Management		
🥗 Event Management	Device	e Arming Control
🔂 Storage Schedule	Founding Bandes Deputite Control De	
🯯 Account Management	Encoding Device Security Control Pa	
🛗 Log Search	☑ All	Arming Status
🕵 System Configuration	✓ 10.7.165.210	
📢 Broadcast		
😝 Device Arming Control		
Alarm Output Control		
Batch Wiper Control		
🕑 Batch Time Sync		
Player		
Message Queue		

2. Click the alarm device to make it in the state of arming.

Pop-up Window Operation

When the window pops up, you can

click	to answer the alarm calling or service consulting;
click 🎿	to reject the alarm calling or service consulting;
click	to hold on the calling or consulting;
click	to turn on electric lock of alarm bar;
click 🚇	to turn on alarm lamp (applicable to panic alarm station with camera);



Panic Alarm Station• User Manual

4.4 Broadcast Settings

Steps:

1. Click **Tool > Broadcast** to enter the broadcast management interface.



- 2. Click the corresponding item.
- 3. (Optional) Unclick the corresponding item if you want to cancel the broadcast.
- 4. Click **Save** to save the setting.

After the broadcast setting, the client can broadcast to multiple devices.

UD09784B

