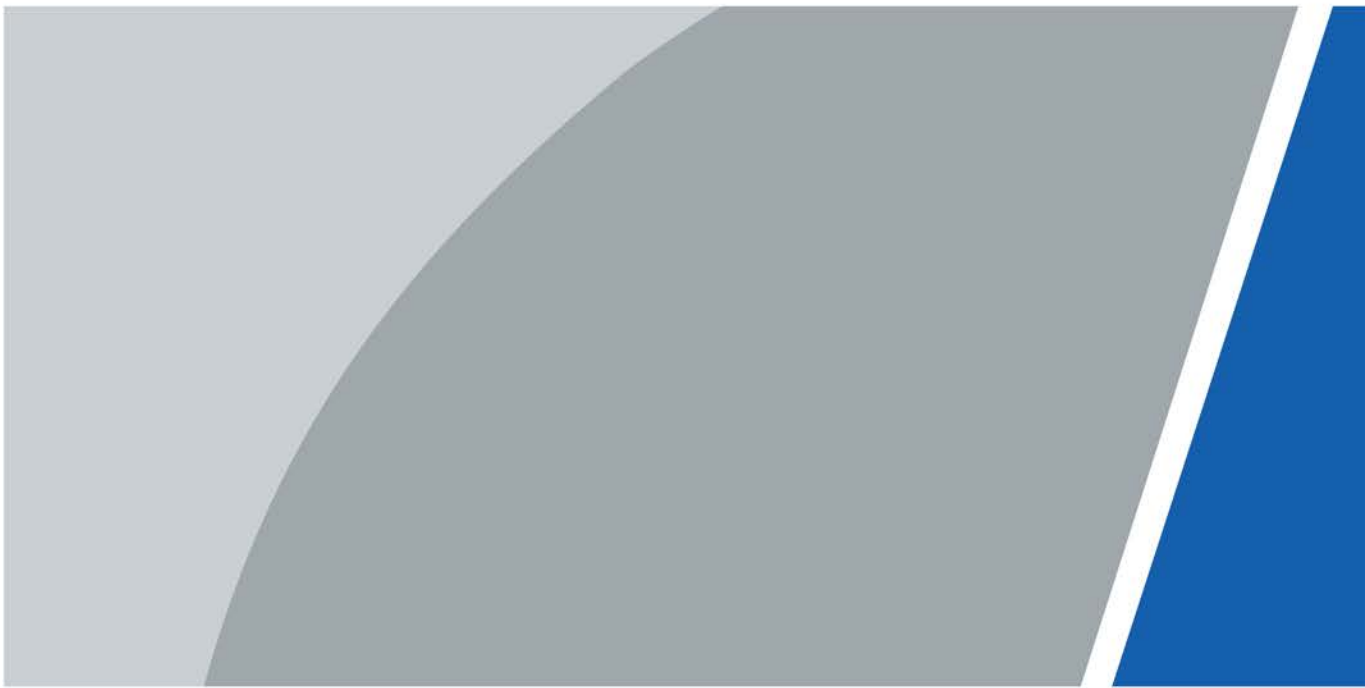


# IVSS for Extreme-C

## User's Manual



# Foreword

## General

The user's manual (hereinafter referred to as "the manual") describes the structure, function and operation of the intelligent video surveillance server (hereinafter referred to as "the Device").

## Models






Number of HDDs	Models
16	IVSS7016DR-4M/G
24	IVSS7024DR-16M/G



- In the model name, R indicates that the model has redundant power.
- In the model name, D indicates that the model has an LCD screen.

## Safety Instruction

The following categorized signal words with defined meaning might appear in the manual.

Signal Words	Meaning
 <b>DANGER</b>	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 <b>WARNING</b>	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 <b>CAUTION</b>	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 <b>TIPS</b>	Provides methods to help you solve a problem or save you time.
 <b>NOTE</b>	Provides additional information as the emphasis and supplement to the text.

## Revision History

Version	Revision Content	Release Time
V1.0.1	<ul style="list-style-type: none"><li>• Updated Important Safeguards and Warnings.</li><li>• Added Particulate and Gaseous Contamination Specifications.</li></ul>	March 2022
V1.0.0	First release.	April 2021

## About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product.
- We are not liable for any loss caused by the operations that do not comply with the manual.

- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, see our final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

# Important Safeguards and Warnings

This section introduces content covering the proper handling of the Device, hazard prevention, and prevention of property damage. Read carefully before using the Device, comply with the guidelines when using it, and keep the manual safe for future reference.

## Operation Requirements



- This is a class A product. In a domestic environment this may cause radio interference in which case you may be required to take adequate measures.
- The Device is heavy and needs to be carried by several persons together to avoid personal injuries.



- Check whether the power supply is correct before use.
- Do not unplug the power cord on the side of the Device while the adapter is powered on.
- Operate the Device within the rated range of power input and output.
- Use the Device under allowed humidity and temperature conditions.
- Do not drop or splash liquid onto the Device, and make sure that there is no object filled with liquid on the Device to prevent liquid from flowing into it.
- Do not disassemble the Device without professional instruction.
- Your configurations will be lost after performing a factory reset. Please be advised.
- Do not restart, shut down or disconnect the power to the Device during an update.
  - ◇ Make sure the update file is correct because an incorrect file can result in a Device error occurring.
  - ◇ The system cannot upgrade different types of AI modules at the same time.
- Do not frequently turn on/off the Device. Otherwise, the product life might be shortened.
- Back up important data on a regular basis when using the Device.
- Operating temperature: 0 °C to 45 °C (32 °F to 113 °F).
- Salt spray in the operating environment of the device might corrode its electronic components and cables. To ensure the normal operation of the device and prolong its service life, use the device in an indoor environment that is 3 kilometers away from the sea.

## Installation Requirements



- Do not connect the power adapter to the Device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Device.
- Do not expose the battery to environments with extremely low air pressure, or extremely high or low temperatures. Also, it is strictly prohibited for the battery to be thrown into a fire or furnace, and to cut or put mechanical pressure on the battery. This is to avoid the risk of fire and explosion.
- Use the standard power adapter or cabinet power supply. We will assume no responsibility for any injuries or damages caused by the use of a nonstandard power adapter.



- Do not place the Device in a place exposed to sunlight or near heat sources.
- Keep the Device away from dampness, dust, and soot.
- Put the Device in a well-ventilated place, and do not block its ventilation.
- Install the server on a stable surface to prevent it from falling.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Note that the power supply requirements are subject to the Device label.
- The Device is a class I electrical appliance. Make sure that the power supply of the Device is connected to a power socket with protective earthing.
- Use power cords that conform to your local requirements, and are rated specifications.
- Before connecting the power supply, make sure the input voltage matches the server power requirement.
- When installing the Device, make sure that the power plug and appliance coupler can be easily reached to cut off power.
- Install the server in an area that only professionals can access.
- Extra protection is necessary for the Device casing to reduce the transient voltage to the defined range.
- If you did not push the HDD box to the bottom, then do not close the handle to avoid damage to the HDD slot.
- Install the Device near a power socket for emergency disconnect.
- It is prohibited for non-professionals and unauthorized personnel to open the Device casing.
- Affix the Device securely to the building before use.

## Maintenance Requirements



- Make sure to use the same model when replacing the battery to avoid fire or explosion. Dispose the battery strictly according to the instructions on it.
- Power off the Device before maintenance.



- AI module does not support hot plug. If you need to install or replace the AI module, unplug the Device power cord first. Otherwise, it will lead to file damage on the AI module.
- The Device casing provides protection for internal components. Use a screwdriver to loosen the screws before detaching the casing. Make sure to put the casing back on and secure it in its original place before powering on and using the Device.
- It is prohibited for non-professionals and unauthorized personnel to open the Device casing.
- The appliance coupler is a disconnection Device. Keep it at a convenient angle when using it. Before repairing or performing maintenance on the Device, first disconnect the appliance coupler.

## Transportation Requirements



Transport the Device under allowed humidity and temperature conditions.

## Storage Requirements



Store the Device under allowed humidity and temperature conditions.

# Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Overview .....	1
1.1 Introduction.....	1
1.2 Login Mode .....	1
2 The Grand Tour .....	2
2.1 16-HDD Series.....	2
2.1.1 Front Panel .....	2
2.1.2 Rear Panel.....	3
2.1.3 Dimensions.....	5
2.2 24-HDD Series .....	5
2.2.1 Front Panel .....	5
2.2.2 Rear Panel.....	6
2.2.3 Dimensions.....	8
3 Hardware Installation .....	9
3.1 Installation Flow .....	9
3.2 Unpacking the Box.....	9
3.3 HDD Installation.....	9
3.4 Cable Connection.....	11
3.4.1 Alarm Connection .....	11
3.4.1.1 Connection .....	11
3.4.1.2 Alarm Port .....	12
3.4.1.3 Alarm Input.....	12
3.4.1.4 Alarm Output.....	13
3.4.2 Connection Diagram.....	14
4 Starting IVSS.....	15
5 Initial Settings.....	16
5.1 Initializing Device.....	16
5.2 Quick Settings.....	18
5.2.1 Configuring IP Address.....	18
5.2.2 Configuring P2P Settings .....	20
5.3 Login.....	21
5.3.1 Logging in to PCAPP Client.....	21
5.3.2 Logging in to Local Interface.....	23
5.3.2.1 Preparation .....	24
5.3.2.2 Operation Steps.....	24

5.3.3 Logging in to Web Interface .....	24
6 System Configuration .....	25
6.1 Configuration Page .....	25
6.2 Network Management .....	25
6.2.1 Basic Network .....	26
6.2.1.1 Configuring IP Address .....	26
6.2.1.2 Port Aggregation .....	27
6.2.1.2.1 Binding NIC .....	28
6.2.1.2.2 Cancelling Binding NIC .....	30
6.2.1.3 Setting Port Number .....	30
6.2.2 Network Apps .....	31
6.2.2.1 UPnP .....	31
6.2.2.2 Multicast .....	32
6.3 Event Management .....	33
6.3.1 Alarm Actions .....	33
6.3.1.1 Buzzer .....	33
6.3.1.2 Log .....	34
6.3.1.3 Email .....	34
6.3.1.4 Local Alarm Out .....	34
6.3.1.5 Voice Prompt .....	35
6.3.2 Local Device .....	35
6.3.2.1 Abnormal Event .....	35
6.3.2.2 Configuring AI Module Slot Number .....	36
6.4 Storage Management .....	37
6.4.1 Local Hard Disk .....	38
6.4.1.1 Viewing S.M.A.R.T .....	38
6.4.1.2 Format .....	39
6.4.1.3 File System Repair .....	39
6.4.1.4 Setting Storage Strategy .....	39
6.4.1.5 Viewing RAID Group .....	40
6.4.2 RAID .....	40
6.4.2.1 Creating RAID .....	41
6.4.2.1.1 Creating RAID .....	41
6.4.2.1.2 Operation .....	44
6.4.2.2 Creating Hot Spare HDD .....	45
6.4.3 Network Hard Disk .....	47
6.4.3.1 iSCSI Application .....	47
6.4.3.2 iSCSI Management .....	47
6.5 Video Recording .....	49



<b>6.6 Security Strategy</b> .....	50
<b>6.6.1 HTTPS</b> .....	50
<b>6.6.1.1 Installing Certificate</b> .....	50
<b>6.6.1.1.1 Installing the Created Certificate</b> .....	50
<b>6.6.1.1.2 Installing Signature Certificate</b> .....	51
<b>6.6.1.2 Enabling HTTPS</b> .....	52
<b>6.6.1.3 Uninstalling the Certificate</b> .....	53
<b>6.6.2 Configuring Access Permission</b> .....	53
<b>6.6.3 Safety Protection</b> .....	54
<b>6.6.4 Enabling System Service Manually</b> .....	55
<b>6.6.5 Configuring Firewall</b> .....	57
<b>6.6.6 Configuring Time Synchronization Permission</b> .....	57
<b>6.7 Account Management</b> .....	58
<b>6.7.1 User Group</b> .....	58
<b>6.7.1.1 Adding User Group</b> .....	59
<b>6.7.1.2 Deleting User Group</b> .....	60
<b>6.7.2 Device User</b> .....	60
<b>6.7.2.1 Adding a User</b> .....	60
<b>6.7.2.2 Operation</b> .....	62
<b>6.7.3 Password Maintenance</b> .....	62
<b>6.7.3.1 Modifying Password</b> .....	62
<b>6.7.3.1.1 Modifying Password of the Current User</b> .....	62
<b>6.7.3.1.2 Modifying Password of Other User</b> .....	63
<b>6.7.3.2 Resetting Password</b> .....	64
<b>6.7.3.2.1 Leaving Email Address and Security Questions</b> .....	64
<b>6.7.3.2.2 Resetting Password on Local Interface</b> .....	64
<b>6.7.4 ONVIF</b> .....	67
<b>6.7.4.1 Adding ONVIF User</b> .....	67
<b>6.7.4.2 Deleting ONVIF User</b> .....	68
<b>6.8 System Configuration</b> .....	69
<b>6.8.1 Setting System Parameters</b> .....	69
<b>6.8.2 System Time</b> .....	70
<b>6.8.3 Display</b> .....	71
<b>6.9 IPSAN</b> .....	72
<b>6.9.1 Creating Storage Pool</b> .....	73
<b>6.9.2 Managing Share Account</b> .....	74
<b>6.9.3 Configuring Share Folder</b> .....	75
<b>6.9.4 Share Control</b> .....	77
<b>7 System Maintenance</b> .....	78

7.1 Overview.....	78
7.2 System Resources.....	79
7.2.1 Viewing Device Information .....	79
7.2.2 Viewing AI Module Information.....	80
7.3 System Information.....	80
7.3.1 Viewing Legal Information .....	80
7.3.2 Viewing Algorithm Version.....	80
7.4 Logs.....	81
7.4.1 Log Classification.....	81
7.4.2 Log Search .....	81
7.4.3 Operation .....	82
7.5 Intelligent Diagnosis .....	82
7.5.1 Run Log .....	82
7.5.2 One-click Export.....	83
7.6 Online User.....	83
7.7 Device Maintenance .....	83
7.7.1 Upgrading Device .....	84
7.7.1.1 Upgrading the Device .....	84
7.7.1.2 Viewing AI module.....	84
7.7.2 Default .....	84
7.7.3 Automatic Maintenance.....	85
7.7.4 IMP/EXP .....	86
8 PCAPP Introduction .....	87
8.1 Interface Description.....	87
8.2 History Record .....	87
8.3 Viewing Downloads .....	87
8.4 Configuring PCAPP.....	88
8.5 Viewing Version Details .....	89
9 Log Out, Reboot, Shut Down, Lock.....	90
10 FAQ.....	92
Appendix 1 Mouse and Keyboard Operations .....	93
Appendix 1.1 Mouse Operations.....	93
Appendix 1.2 Virtual Keyboard.....	93
Appendix 2 RAID.....	96
Appendix 3 HDD Capacity Calculation .....	98
Appendix 4 Glossary .....	99
Appendix 5 Particulate and Gaseous Contamination Specifications .....	101
Appendix 5.1 Particulate Contamination Specifications .....	101
Appendix 5.2 Gaseous Contamination Specifications .....	101



# 1 Overview

## 1.1 Introduction

As an intelligent video surveillance server (hereinafter referred to as IVSS or the Device), IVSS delivers not only the basic video surveillance functions, but also a bunch of advanced AI features such as face recognition and video metadata, providing AI-based all-in-one surveillance solution for customers.

- General functions: Video surveillance, video storage, alarm, record search and playback, intelligent analysis features.
- User-friendly interface.
- 4K and H.265 decoding.
- Applicable to scenarios such as intelligent building, large parking lot, financial planning area and more.

## 1.2 Login Mode

You can operate the device by using the local interface, web client and PCAPP client (the PC client, hereinafter referred to as PCAPP).



Operation and system configuration in this manual is mainly based on PCAPP. There might be differences from local or web operation.

Table 1-1 Login mode

Login Mode	Operation	Description
Local login	Connect the display, mouse and keyboard to the device. View and operate the local menu on the display.	Support all functions of the device.
Web login	Connect the device and PC into the same network, and remotely access the device through browser (Google Chrome and Firefox) on PC.	Support majority functions of the device, except live, record playback and video-related function.
Log in PCAPP	Connect the device and PC into the same network, download and install PCAPP on PC, and then remotely access the device with PCAPP.	Support all functions of the device.

## 2 The Grand Tour

This section introduces front panel, rear panel, port function and button function, indicator light status, and so on.

### 2.1 16-HDD Series



- The Device has an embedded display on select models.
- The Device has power redundancy on select models.

#### 2.1.1 Front Panel

Figure 2-1 Front panel with LCD

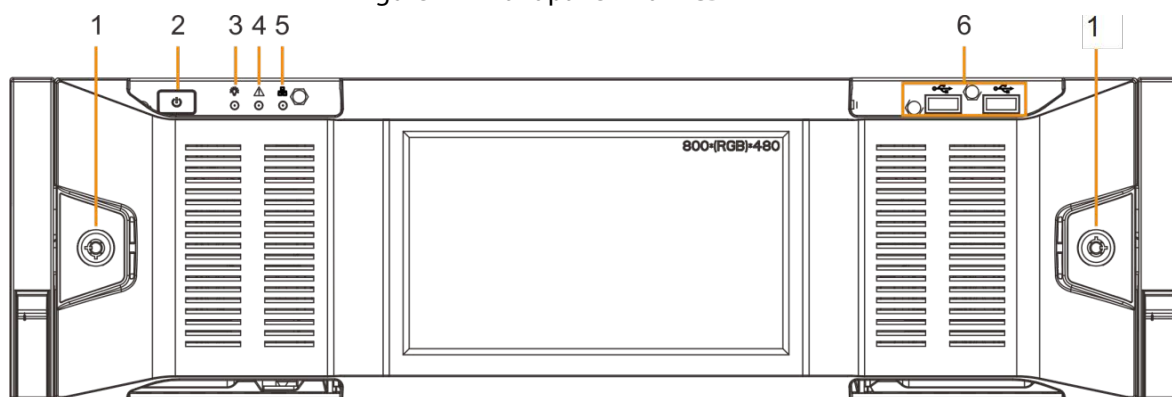


Table 2-1 Front panel description

No.	Button/Port	Description
1	Front panel lock	Once the front panel lock is secure, it can prevent HDD from being stolen or removed by mistake. Unlock the front panel lock and remove the front panel, you can view 16 HDD slots.
2	Power	Boot up or shut down device. The power on-off button has the indicator light. It can display device-running status. <ul style="list-style-type: none"> <li>• When device is off (indicator light is off), press the button for a short period to boot up device.</li> <li>• When device is running, (blue indicator light is on), press the button for at least 4 seconds to shut down the device.</li> </ul>
3	System status indicator light	Displays the system running status. <ul style="list-style-type: none"> <li>• The blue light is on: Device is running properly.</li> <li>• The indicator light is off: The device is not running.</li> </ul>
4	Alarm indicator light	Displays local input alarm status. <ul style="list-style-type: none"> <li>• Red indicator light is on: There is local alarm input event.</li> <li>• The indicator light is off: There is no local alarm input event.</li> </ul>

No.	Button/Port	Description
5	Network indicator light	Displays current network status. <ul style="list-style-type: none"> <li>The indicator light is blue: It means at least one Ethernet port has connected to the network.</li> <li>The indicator light is off: No Ethernet ports are connected to the network.</li> </ul>
6	USB port	Connects to external devices such as USB storage device, keyboard and mouse.

## 2.1.2 Rear Panel

Figure 2-2 IVSS7016-M rear panel (redundant power)

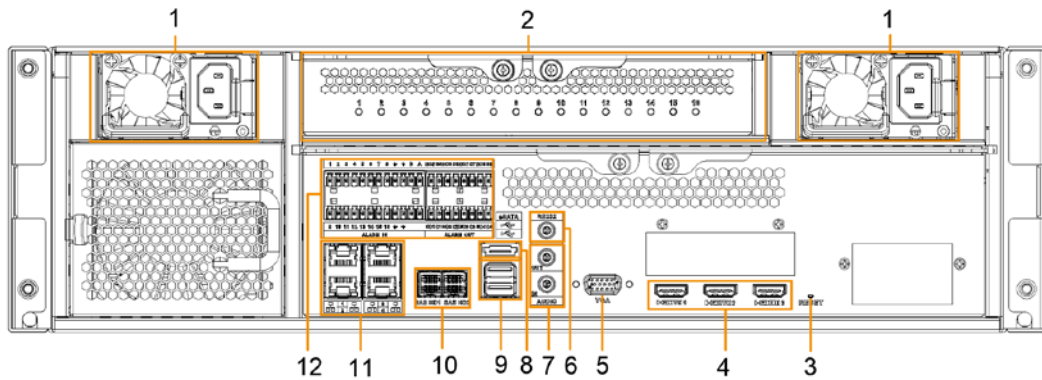



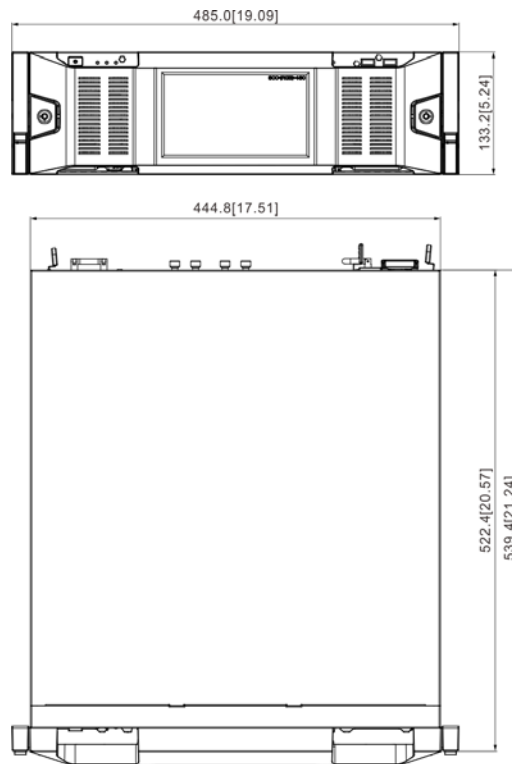
Table 2-2 IVSS7016 rear panel description

No.	Name	Description
1	Power input port	Inputs 100-240 VAC power.
2	AI module indicator light	Displays AI module status. <ul style="list-style-type: none"> <li>The yellow light flashes: AI module is running properly.</li> <li>The yellow light is on: AI module is malfunctioning.</li> </ul>  This function is valid if there is AI module.
3	RESET button	Reserved.
4	HDMI port	High definition audio and video signal output port. The port outputs the uncompressed high definition video and multi-channel audio data to the connected display with HDMI port. The three HDMI ports are different source output.
5	VGA port	VGA video output port. It outputs analog video signal. The VGA port and HDMI 1 port are same source output.
6	RS-232 port	RS-232 COM debug. It is used for general COM debug, setting IP address, and transmitting transparent COM data.
7	AUDIO IN	Audio input port

No.	Name	Description
	AUDIO OUT	Audio output port
8	eSATA port	SATA peripheral port. Connects to SATA port or eSATA device.
9	USB port	Connects to external devices such as USB storage device, keyboard and mouse.
10	SAS port	SAS extension port. It can connect to the SAS extension controller.
11	Network port	10/100/1000 Mbps self-adaptive Ethernet port. Connects to the network cable.
12	Alarm Input	<p>16 groups (1–16) alarm input ports. They are corresponding to ALARM 1–ALARM 16. The alarm becomes valid in low level.</p> <ul style="list-style-type: none"> <li>• A and B: Control the A/B cable of the RS–485 device. It is used to connect to the PTZ camera. Please connect 120 Ω between A/B cables if there are too many PTZ decoders.</li> <li>• <math>\perp</math>: GND end.</li> </ul>
	Alarm Output	<p>8 groups of alarm output ports (NO1 C1–NO8 C8). They output alarm signal to the alarm device. Please make sure there is power to the external alarm device.</p> <ul style="list-style-type: none"> <li>• NO: Alarm output port of Normally Open type.</li> <li>• C: Common alarm output port.</li> <li>• <math>\perp</math>: GND end.</li> </ul>

## 2.1.3 Dimensions

Figure 2-3 Dimensions with LCD (mm [inch])



## 2.2 24-HDD Series

### 2.2.1 Front Panel

Figure 2-4 Front panel with LCD

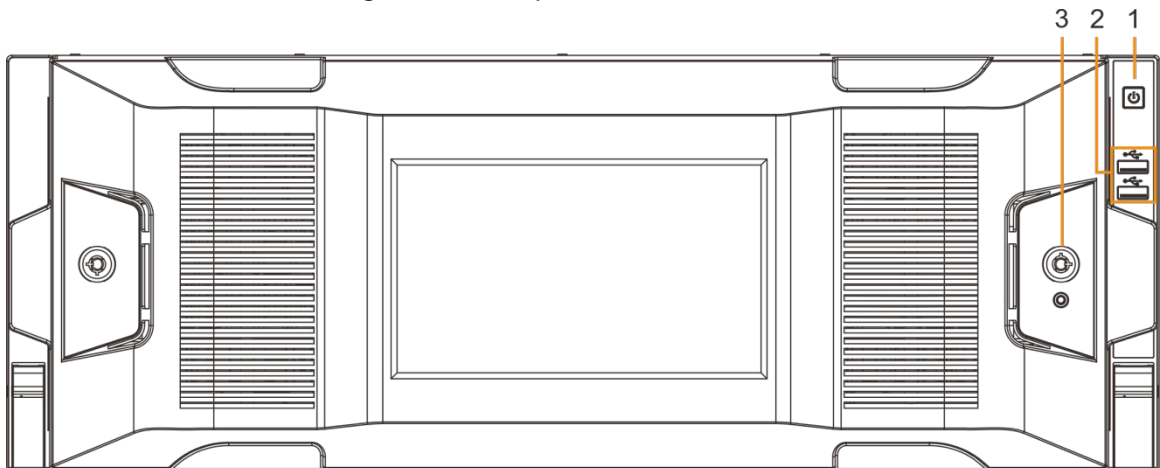




Table 2-3 Front panel description

No.	Button/Port	Description
1	Power on-off button	<p>Boot up or shut down device. The power on-off button has the indicator light. It can display device-running status.</p> <ul style="list-style-type: none"> <li>When device is off (indicator light is off), press the button for a short period to boot up device.</li> <li>When device is running, (blue indicator light is on), press the button for at least 4 seconds to shut down the device.</li> </ul>
2	USB port	Connects to external devices such as USB storage device, keyboard and mouse.
3	Front panel lock	Once the front panel lock is secure, it can prevent HDD from being stolen or removed by mistake. Unlock the front panel lock and remove the front panel, you can view 16 HDD slots.

## 2.2.2 Rear Panel

Figure 2-5 IVSS7024-M rear panel (redundant power)

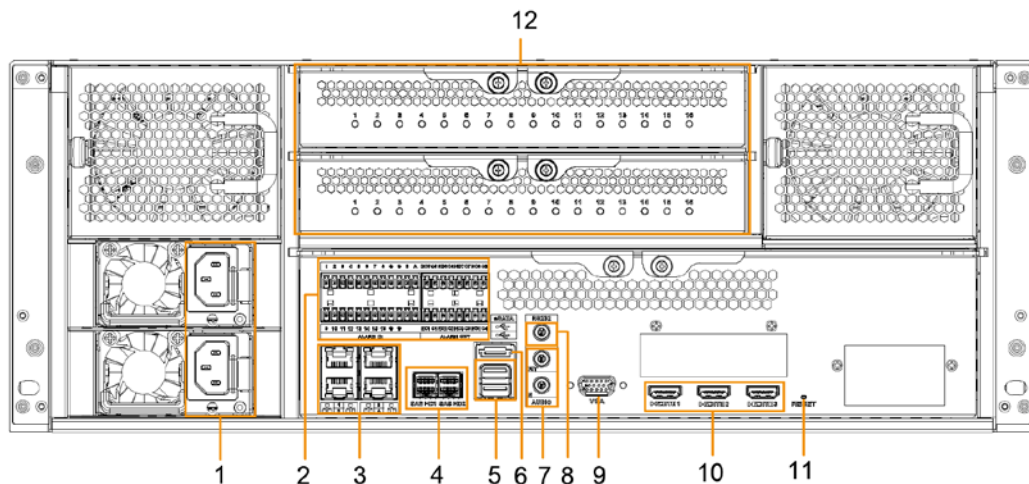



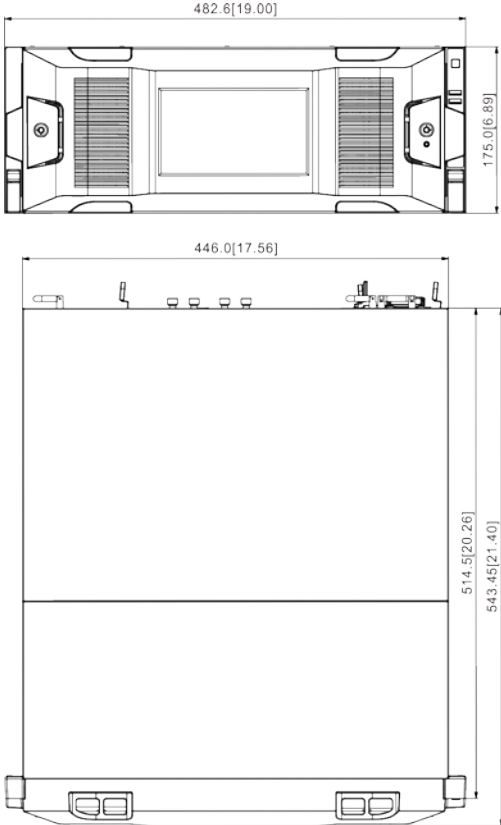
Table 2-4 IVSS7024 rear panel description

No.	Button/Port	Description
1	Power input port	Inputs 100-240 VAC power.
2	Alarm Input	<p>16 groups (1–16) alarm input ports. They are corresponding to ALARM 1–ALARM 16. The alarm becomes valid in low level.</p> <ul style="list-style-type: none"> <li>A and B: Control the A/B cable of the RS-485 device. It is used to connect to the PTZ camera. Please connect 120 Ω between A/B cables if there are too many PTZ decoders.</li> <li>⏏: GND end.</li> </ul>

No.	Button/Port	Description
	Alarm Output	<p>8 groups of alarm output ports (NO1 C1–NO8 C8). They output alarm signal to the alarm device. Please make sure there is power to the external alarm device.</p> <ul style="list-style-type: none"> <li>• NO: Alarm output port of Normally Open type.</li> <li>• C: Common alarm output port.</li> <li>• <math>\perp</math>: GND end.</li> </ul>
3	Network port	10/100/1000 Mbps self-adaptive Ethernet port. Connects to the network cable.
4	SAS port	SAS extension port. It can connect to the SAS extension controller.
5	USB port	Connects to external devices such as USB storage device, keyboard and mouse.
6	eSATA port	SATA peripheral port. Connects to SATA port or eSATA device.
7	AUDIO IN	Audio input port
	AUDIO OUT	Audio output port
8	RS-232 port	RS-232 COM debug. It is used for general COM debug, setting IP address, and transmitting transparent COM data.
9	VGA port	VGA video output port. It outputs analog video signal. The VGA port and HDMI 1 port are same source output.
10	HDMI port	High definition audio and video signal output port. The port outputs the uncompressed high definition video and multi-channel audio data to the connected display with HDMI port. The three HDMI ports are different source output.
11	RESET button	Reserved.
12	AI module indicator light	<p>Displays AI module status.</p> <ul style="list-style-type: none"> <li>• The yellow light flashes: AI module is running properly.</li> <li>• The yellow light is on: AI module is malfunctioning.</li> </ul> <p> This function is not available without AI module.</p>

# 2.2.3 Dimensions

Figure 2-6 Dimensions with LCD (mm [inch])



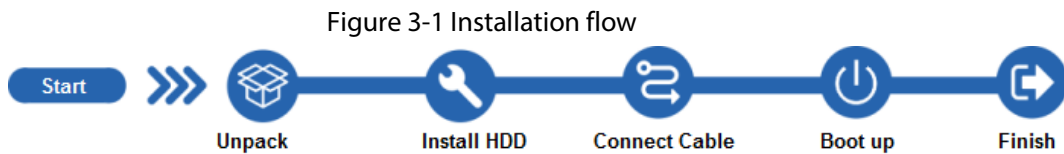
# 3 Hardware Installation

This section introduces HDD installation, cable connection, and so on.



Some series product is heavy. It needs several persons to carry or move, in order to prevent person injury.

## 3.1 Installation Flow



## 3.2 Unpacking the Box

When you receive IVSS, please check against the following checking list. If any of the items are missing or damaged, contact the local retailer or after-sales engineer immediately.

No.	Button/Port		Content
1	Whole package	Appearance	Check whether there is any visible damage.
		Package	Check whether there is any accidental clash during transportation.
		Accessories (list of accessories on the warranty card)	Check whether they are complete.
2	Device	Appearance	Check whether there is any visible damage.
		Device model	Check whether the model is the same as order contract.
		The label on the device	Check whether it is torn or not. Do not tear off, or discard the label. Usually you need to show the serial number when we provide after-sales service.

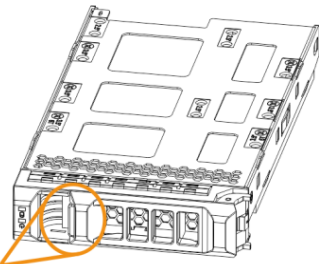
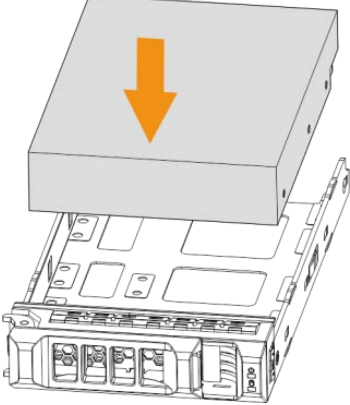
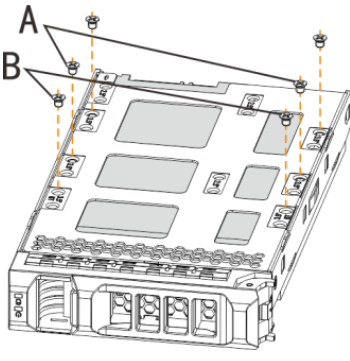

## 3.3 HDD Installation

The section introduces the detailed operations to install HDD.

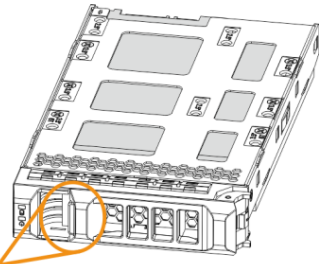
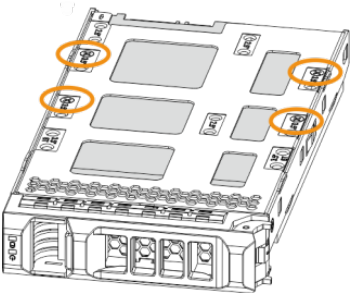
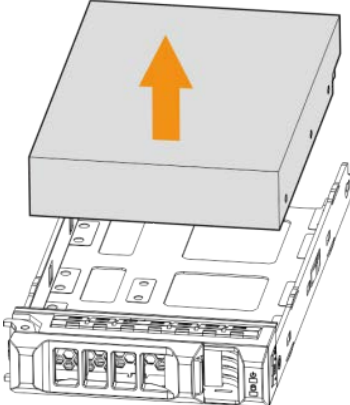



- Different models support different HDD numbers.
- If you have not pushed the HDD box to the bottom, do not close the handle to avoid any damage to the HDD slot.

## Installing HDD

 <p>Button</p>		
<p>① Press the button on the front panel of IVSS, open the handle, and then pull out the HDD box.</p>	<p>② Put the HDD into the box along the direction shown in the figure.</p>	<p>③ Lock the screws on the back of the HDD box. Insert the box into the HDD slot, push it to the bottom, and then close the handle.</p> <p> In the figure, you only need to lock one set of the screws (Group A or Group B). See the actual situation.</p>

## Removing HDD

 <p>Button</p>		
<p>① Press the button on the front panel of IVSS, open the handle, and then pull out the HDD box.</p>	<p>② Unlock the screws on the back of the HDD box.</p> <p> The screws are at different positions for different HDDs.</p>	<p>③ Take out the HDD and reinsert the box to the slot. Push it to the bottom and close the box handle.</p>

## 3.4 Cable Connection

The section introduces cable connection of IVSS.

### 3.4.1 Alarm Connection

Before using the alarm, connect alarm input or alarm output device.

#### 3.4.1.1 Connection

The section introduces alarm connection of IVSS.

##### Alarm Input

- Both NO and NC are supported.
- The alarm input port supports alarm signal from ground and device of 12-24 V voltage.
- If the alarm device is connected to the Device and other devices, use relay for isolation.

##### Alarm Output

The alarm output port cannot be connected to high-power load (less than 1 A). When forming output circuit, the excessive current should be prevented from causing damage to the relay. Use the contactor for isolation when applying high-power loads.

##### PTZ Decoder Connection

- The common-ground must be prepared for PTZ decoder and the Device; otherwise the common-mode voltage might not be able to control the PTZ. It is recommended to use shielded twisted pair, and the shielding layer can be used for common ground.
- Prevent interference from high-voltage power, make reasonable wiring, and take measures for lightning protection.
- Remotely import 120  $\Omega$  to reduce resistance reflection and protect the signal quality.
- The Device A line and B line cannot connect to other RS-485 output device in parallel.
- The voltage between the A line and B line of PTZ decoder must be less than 5 V.

##### Notes to Grounding

- Poor grounding of camera might damage the chip.
- When supplying external power source to the alarm device, the alarm device should be common-grounded with IVSS.

### 3.4.1.2 Alarm Port

Figure 3-2 Alarm port (IVSS7016/IVSS7024)

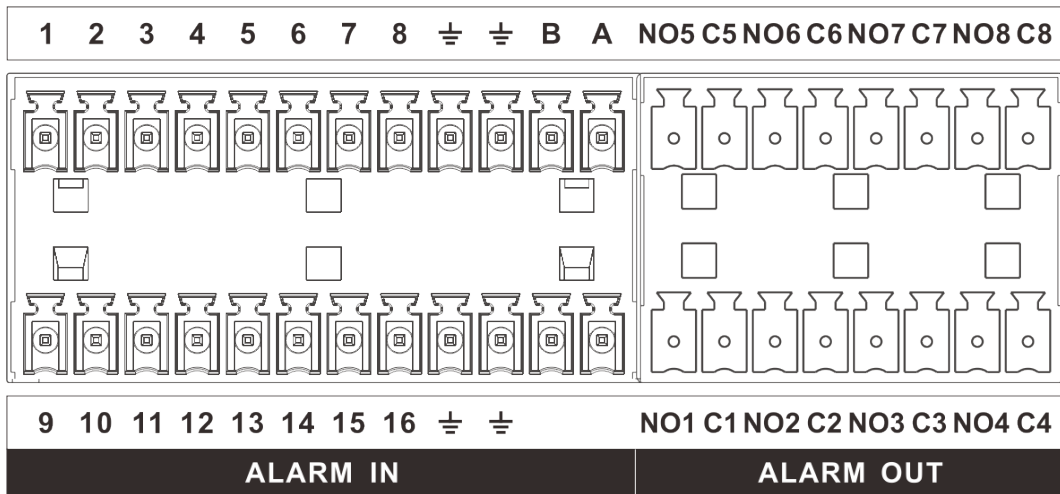


Table 3-1 Alarm port

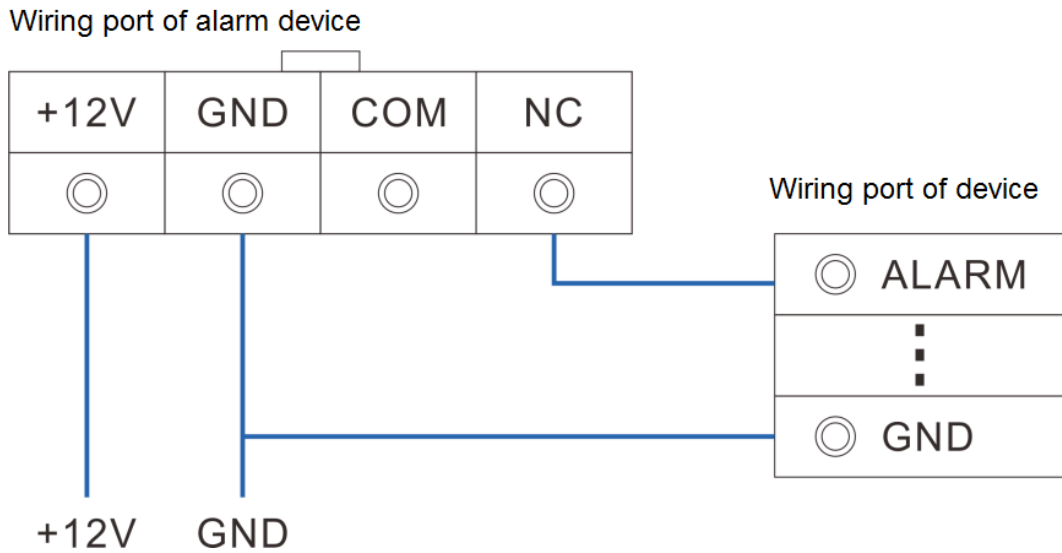
Icon	Description
1–16	They are corresponding to ALARM 1–ALARM 16. The alarm becomes valid in low level.
NO1 C1–NO8 C8	Eight groups of normally open linkage output (on-off value)
⏏	Grounding wire.
A, B	A and B: Control the A/B cable of the RS–485 device. It is used to connect to the PTZ camera. Please parallel connect 120 Ω between A/B cables if there are too many PTZ decoders.

### 3.4.1.3 Alarm Input

Both NO and NC are supported. For connection of NC alarm input port, see the following figures.

- GND and COM of alarm device shall be connected in parallel. Alarm device shall be powered with external power source.
- Connect GND of alarm device with GND of Device in parallel.
- Connect the NC port of alarm device to the alarm input port (1–16).

Figure 3-3 NC alarm input connection



### 3.4.1.4 Alarm Output

- The alarm output is on-off output (Normally Open Contact), and there should be external power supply to alarm output device.
- RS-485 A line and B line: connecting the A line and B line on the PTZ decoder.
- To avoid overload from damaging the Device, see the parameters about relay.

Table 3-2 Relay parameters of alarm output port

Model		HRB1-S-DC5V
Contact material		Silver
Rated value (resistance load)	Rated power capacity	24 VDC 2 A, 125 VAC 2 A
	Maximum power	62.5 VA/30 W
	Maximum power voltage	125 VAC, 60 VDC
	Maximum power current	2 A
Insulation	Between contacts	1,000 VAC 1 minute
	Between contact and loop	400 VAC 1 minute
Insulation voltage		1,000 MΩ (500 VDC)
Turn-on Time		< 5 ms
Turn-off Time		< 5 ms
Life	Mechanical	300 times per1 minute
	Electrical	30 times per1 minute
Operating ambient temperature		-30 °C to +70 °C



## 3.4.2 Connection Diagram

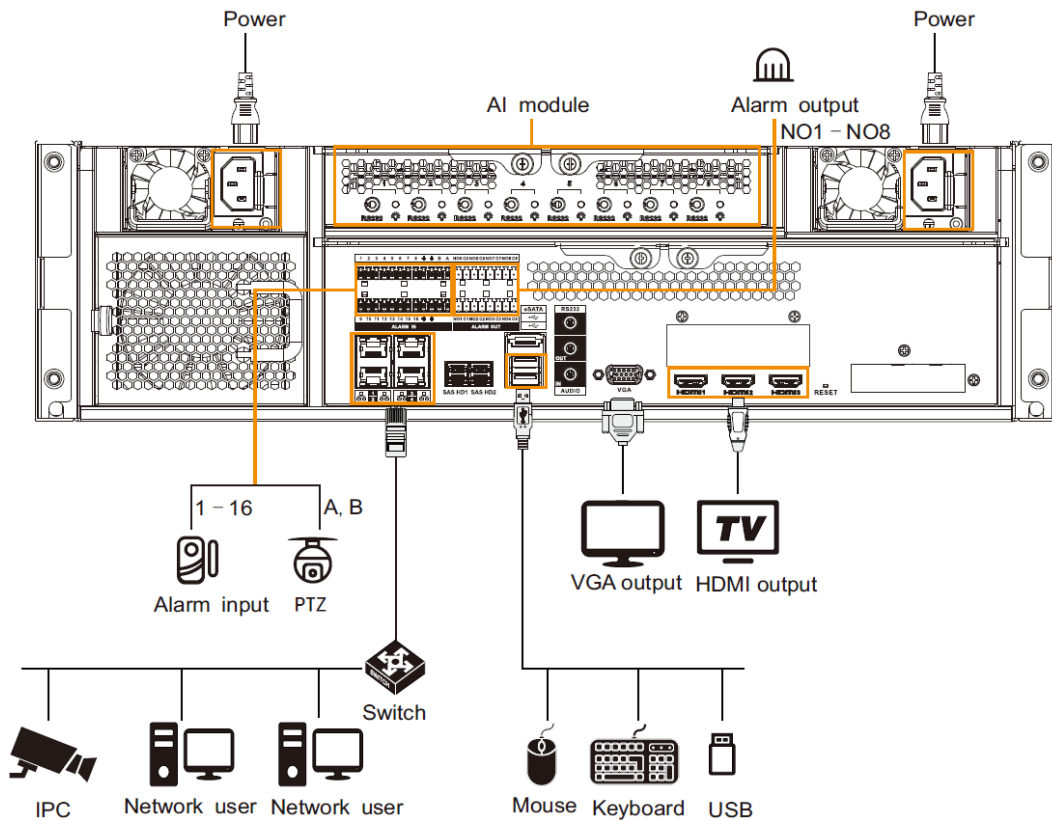


The following steps are to connect 16-HDD series device. See the actual product for detailed information.

The following figure is for reference only.

- Display, mouse and keyboard are needed for local operation.
- Before using the smart detection functions such as face detection and face recognition, you shall install the AI module first.

Figure 3-4 Connection diagram



## 4 Starting IVSS



- Before starting the device, make sure that the input voltage shall match the device power requirement.
- To ensure stable operation of the device and prolong service life of HDD, provide stable voltage with less ripple interference by reference to international standard.
- For device security, connect other cables of the device first, and then connect the device to the power socket.

Boot-up might be different depending on the model you purchased.

- Connect to the power socket to boot up IVSS.
- After clicking shutdown button on the GUI to shut down the Device, press the power button for a short period of time to boot up the Device.

# 5 Initial Settings

When using IVSS for the first time, initialize the device, and set basic information and functions first.

## 5.1 Initializing Device

If it is your first time to use the device after purchasing or after restoring factory defaults, set a login password of admin (system default user). At the same time, you can set proper password protection method.



Take web remote initialization for example.

**Step 1** Open the browser, enter IP address, and then press Enter.



Default IP address of network port 1 to network port 4 are 192.168.1.108 to 192.168.4.108.

Enter the corresponding IP address of the actually connected network port.

**Step 2** On the **Language Set** page, select a country or region, a language, and a language standard. Click **Next**. The language setting step is only available on the local page of the Device.

Figure 5-1 Time setting

Device Initialization

1 Time 2 Input Password 3 Password Protection

Date  
2019-11-04

Time  
10:52:52

Time Zone  
(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi, etc.


Time  
 Manual Setting  
Date/Time 2019-11-04 10:51:35  
 Sync with Internet Time Server  
Server clock.isc.org  
Auto Sync Time Interval 1 hours

Next

**Step 3** On the **Time** page, set time parameters.

Table 5-1 Time parameters description

Parameters	Description
Time Zone	The time zone of the Device.

Parameters	Description
Time	<p>Set system date and time manually or by synchronizing with NTP server time.</p> <ul style="list-style-type: none"> <li>Manual setting: Select date and time from the calendar.</li> <li>Sync with Internet Time Server: Select <b>Sync with Internet Time Server</b>, enter NTP server IP address or domain, and then set the automatic synchronization interval.</li> </ul> <p> Device time will synchronize with the server time after <b>Sync with Internet Time Server</b> is set.</p>

**Step 4** Click **Next**.

Figure 5-2 Set password

The screenshot shows the 'Device Initialization' process at the 'Input Password' step. It features three input fields: 'Username' (with a person icon), 'Password' (with a lock icon, a strength indicator, and a help icon), and 'Confirm Password' (with a lock icon). At the bottom right, there are 'Back' and 'Next' buttons.

**Step 5** Set admin login password.

Table 5-2 Description of password parameters

Parameters	Description
Username	The default user name is admin.
Password	Set admin login password, and confirm the password.
Confirm Password	The new password can be 8 characters to 32 characters in length and contains at least two types from number, letter and special characters (excluding " "; & and space). Enter a strong password according to the password strength indication.

**Step 6** Click **Next**.

Figure 5-3 Password protection

**Step 7** Set password protection information.

You can use the email you input here or answer the security questions to reset admin password. See "6.7.3.2 Resetting Password" for detailed information.



- Click  to cancel the email or security questions.
- If the email or security questions are not set, the password can be reset on the local interface only.

Table 5-3 Password protection

Password protection mode	Description
Email	Enter an email address for resetting password.
Security question	Set security questions and corresponding answers. Reset the password through the security question.

**Step 8** Click **Finish** to complete device initialization.

The device initialization page is displayed. You can add initialized device to platform for management.

## 5.2 Quick Settings

After initializing the device, the system goes to quick settings page. You can quickly set system time, IP address, and P2P.

### 5.2.1 Configuring IP Address

Configure device IP address, DNS server information and other information according to network planning.



Device has 4 Ethernet ports by default. Make sure that at least one Ethernet port has been connected to the network before you set IP address.

**Step 1** On the completion page of initialization, click **Enter Quick Setting**.

Figure 5-4 IP setting

NIC	NIC Type	Dhcp	IP Address	Subnet Mask	Mac	Speed	Operate
Ethernet Netw...	Electric Port	No				10M/100M/1000...	
Ethernet Netw...	Electric Port	No				10M/100M/1000...	
Ethernet Netw...	Electric Port	No				10M/100M/1000...	
Ethernet Netw...	Electric Port	No				10M/100M/1000...	

**DNS Server**

IP Type:

Obtain DNS server address automatically

Use the following DNS server address

Preferred DNS:

Alternate DNS:

**Default NIC**

Default Ethernet:

**Next**

**Step 2** Configure IP address.

- 1) Click of the corresponding NIC.

Figure 5-5 Edit Ethernet network

Speed: 1000 Mb/s

IP Type:

Use Dynamic IP Address

Use Static IP Address

Static IP Address:

Subnet Mask:

Gateway:


MTU:  (1500-7200)

**OK** **Cancel**

- 2) Set parameters.

Table 5-4 TCP/IP parameters description

Parameters	Description
Speed	Current NIC max network transmission speed.

Parameters	Description
IP Type	Select IPv4 or IPv6.
Use dynamic IP address	When there is a DHCP server on the network, check <b>Use Dynamic IP Address</b> , system can allocate a dynamic IP address to the device. There is no need to set IP address manually.
Use static IP address	Check <b>Use Static IP Address</b> , and then set static IP address, subnet mask and gateway to set a static IP address for the device.
MTU	<p>Set NIC MTU value. The default setup is 1500 Byte.</p> <p>We recommend you to check the MTU value of the gateway first and then set the device MTU value equal to or smaller than the gateway value. It is to reduce the packets slightly and enhance network transmission efficiency.</p> <p> Changing MTU value might result in NIC reboot, network offline and affect current running operation. Please be careful!</p>

3) Click **OK**.

Device goes back to **IP Set** page.

**Step 3** Set DNS server information.

You can select to get DNS server manually or input DNS server information.



This step is compulsive if you want to use domain service.

1) Select an IP type for DNS server. You can select IPv4 or IPv6.

2) Select the way of setting DNS IP address.

**Step 4** Set default NIC.

Select default NIC from the drop-down list.



Make sure that the default NIC is online.

**Step 5** Click **Next** to save settings.

## 5.2.2 Configuring P2P Settings

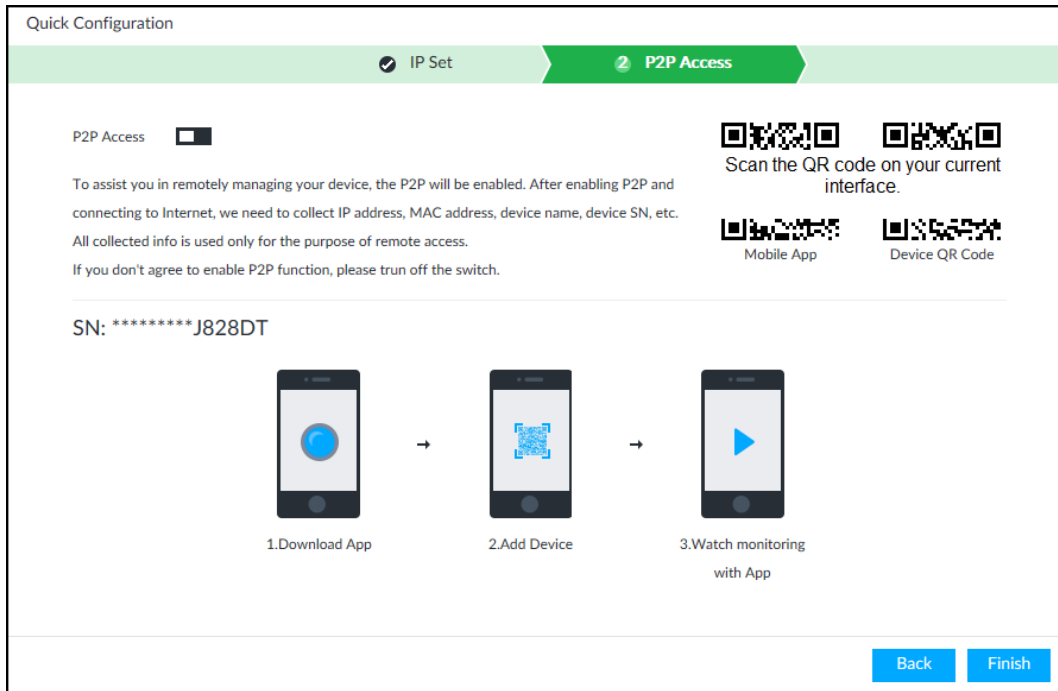
P2P is a peer to peer technology. You can scan the QR code to download cellphone APP without DDNS service or the port mapping or installing the transmission server. After register the device to the APP, you can view the remote video, playback record file and so on.



Make sure that the system has been connected to the network. Otherwise, the P2P function is null.

**Step 1** On **IP Set** page, click **Next**, and then scan the QR code on the actual page.

Figure 5-6 P2P access



Step 2 Click  to enable P2P function. The function is disabled by default.

Step 3 Click **Finish** to save settings.

After the configuration, you can register a device to the APP to view remote video, playback record file, and so on. See corresponding cellphone APP for detailed information.

## 5.3 Login

You can operate the device by using the local interface, web client and PCAPP.

- Display and mouse are needed for local operation.
- Remotely access with web and IPCAPP. PCAPP client is recommended.



After initializing the device, you have logged in by default. Now you can set system settings and operate.

### 5.3.1 Logging in to PCAPP Client

Log in to the PCAPP for system configuration and operation.

Step 1 Download PCAPP.


- 1) Open the browser, enter IP address, and press Enter.
- 2) Click **Download PCAPP** to download PCAPP installation package.

Step 2 Install PCAPP.

- 1) Double-click the installation package.
- 2) Select a language of the PCAPP.
- 3) Click **EULA**, read through the content, and then select the check box of **I Agree EULA**.
- 4) (Optional) Select installation path, click **Custom**, and then select a path.
- 5) Click **Install**.

Step 3 Log in to PCAPP.



- 1) There are two ways to enter PCAPP.
  - On the installation completion page, click **Run**.
  - Double-click the shortcut icon  on the PC desktop.




- When PC theme is not Aero, the system will remind you to switch the theme. To ensure video smoothness, switch your PC to Aero theme. For details, see "8.4 Configuring PCAPP".
- System displays PCAPP at full-screen by default. Click  to display the task column.

Figure 5-7 Prompt

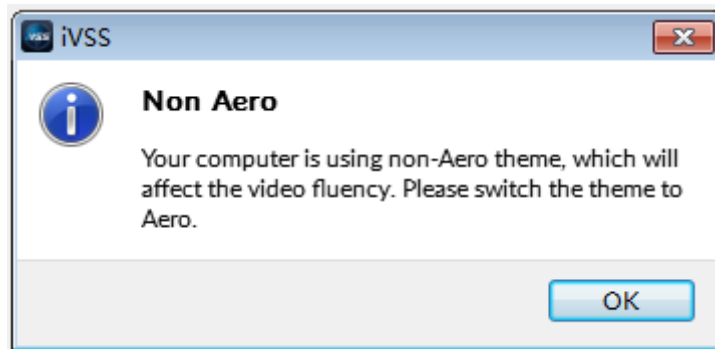



Figure 5-8 Task bar



- 2) Enter device IP address, and then press **Enter** or click .
- 3) Enter device user name and password.



- Click **Login**. For your device safety, change the admin password regularly and keep it well.
  - In case you forgot password, click **Forgot password** to reset.
- 4) Select the login type among TCP, UDP and Multicast. Keep it TCP if you have no special requirement for TCP or UDP.
  - 5) Click **Login**.  
The **LIVE** page is displayed.

Figure 5-9 Live view

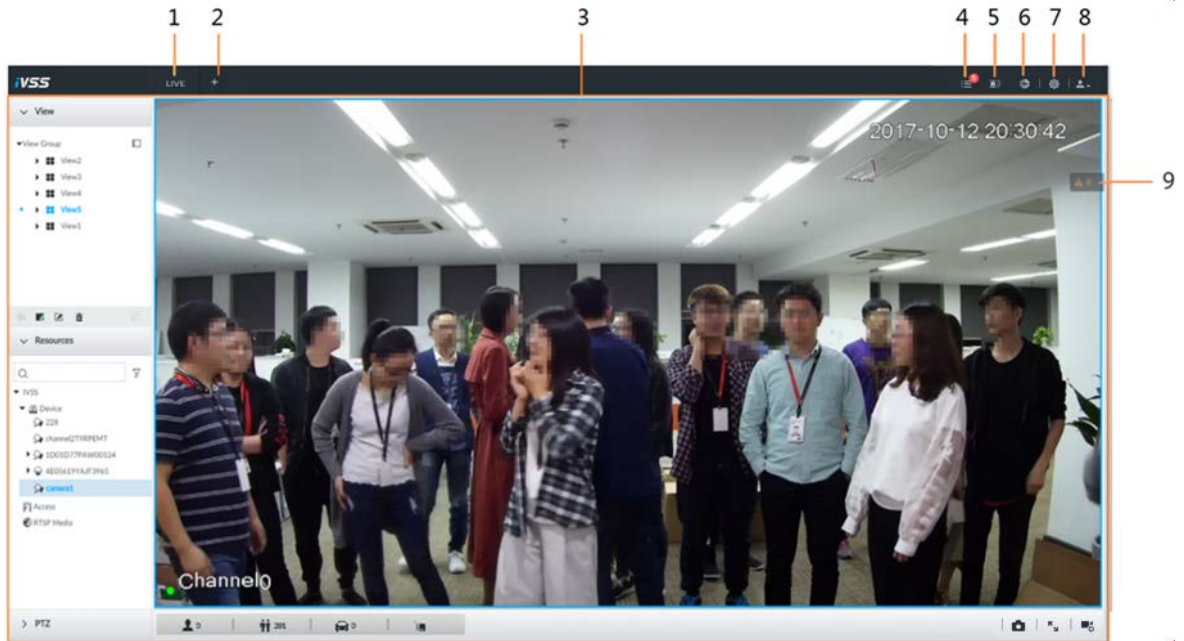





Table 5-5 Home page description

No.	Name	Description
1	Task column	Displays enabled application icon. Move the mouse to the app and then click  to close the app.  The live function is enabled by default and cannot be closed.
2	Add icon	Click to display or hide app page. On app page to view or enable app.
3	Operation area	Displays currently enabled app operation page.
4	System Info	Click to view system information.
5	Buzzer	Click the icon to view buzzer messages.
6	Background Task	Click to view the background running task information.
7	System config	Click to enter system configuration mode.
8	Login user	Click it to change user password, lock user, logout user, reboot device or close device.
9	Alarm list	Click to view the unprocessed alarm event quantity.  Drag this icon to move its position.

### 5.3.2 Logging in to Local Interface

You can view the local page of the Device by connecting a display to it, and then you can carry out local operation on the display.

### 5.3.2.1 Preparation


Ensure that the Device is connected with display, mouse and keyboard. For cable connection, see "3.4 Cable Connection".

### 5.3.2.2 Operation Steps

Step 1 Turn on the Device.


Step 2 Enter user name and password.



- Click **Login**. For your device safety, change the admin password regularly and keep it well.
- Move the mouse to  to view the password prompt information. It is to help you remember password.
- In case you forgot password, click **Forgot Password** to reset. See "6.7.3.2 Resetting Password".

Step 3 Click **Login**.



Click  to control the local screen.

### 5.3.3 Logging in to Web Interface

System supports general browser such as Google Chrome, Firefox to access the web to manage the device remotely, operate and maintain the system.



When you are using general browser to access the web, system supports setting function only. It cannot display the view. It is suggested that PCAPP should be used.

Step 1 Open the browser, input IP address, and press Enter.

Step 2 Enter user name and password.



- Click **Login**. For your device safety, change the admin password regularly and keep it well.
- In case you forgot password, click **Forgot Password** to reset. See "6.7.3.2 Resetting Password" for detailed information.

Step 3 Select the login type among TCP, UDP and Multicast. Keep it TCP if you have no special requirement for TCP or UDP.


Step 4 Click **Login**.

System displays **LIVE** page.


# 6 System Configuration

This chapter introduces system configuration functions such as managing remote device, setting network, setting alarm event, setting HDD storage, managing user information, setting device security strategy, and setting system parameters.

## 6.1 Configuration Page

Click  to open the configuration page.

On this page, you can:

- Click the corresponding app icon to go to the corresponding page. The task column displays current running app name. Move the mouse pointer to the app name and then click  to close the app.
- Click **Exit** to exit the page.

## 6.2 Network Management



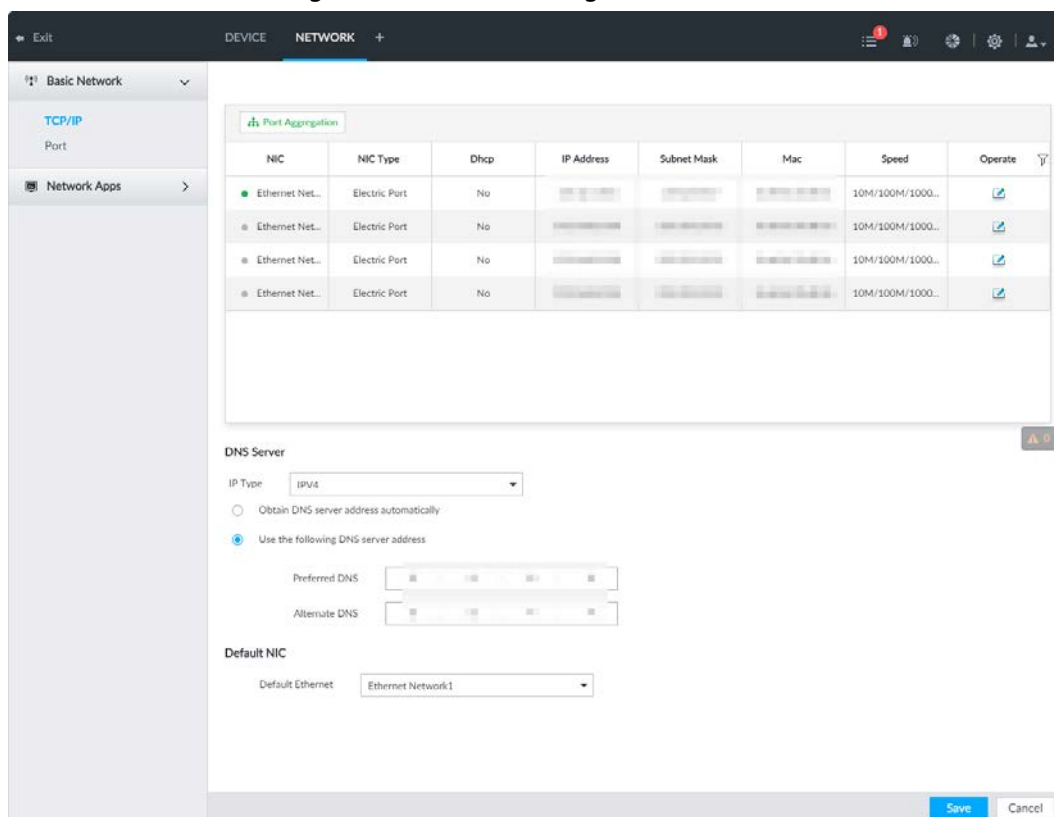
Click  or click  on the configuration page, select **NETWORK**. You can set basic network parameters and application.

Figure 6-1 Network management



## 6.2.1 Basic Network



Set basic network parameters of the device, such as IP address, port aggregation and port number, to connect with other devices in the network.

### 6.2.1.1 Configuring IP Address

Set device IP address, DNS server information and other information according to network planning.



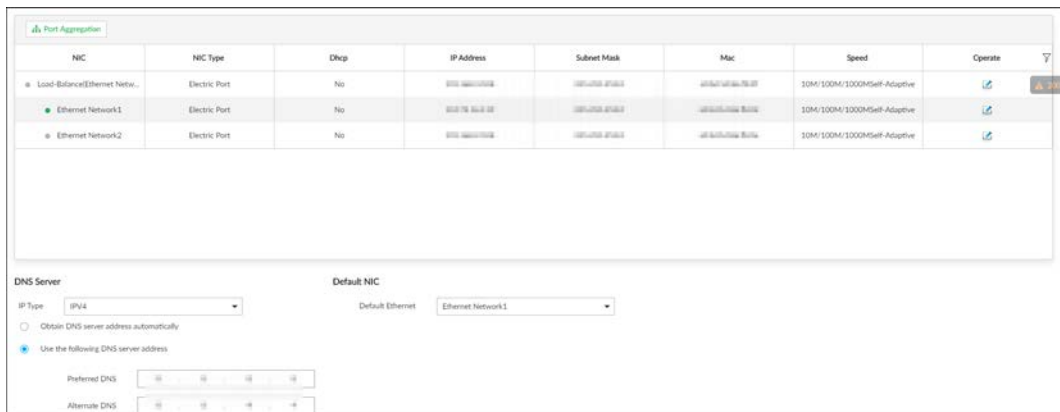
Device has 4 Ethernet ports by default. Make sure that at least one Ethernet port has connected to the network before you set IP address.

**Step 1** Click  or click  on the configuration page, and then select **NETWORK > Basic Network > TCP/IP**.



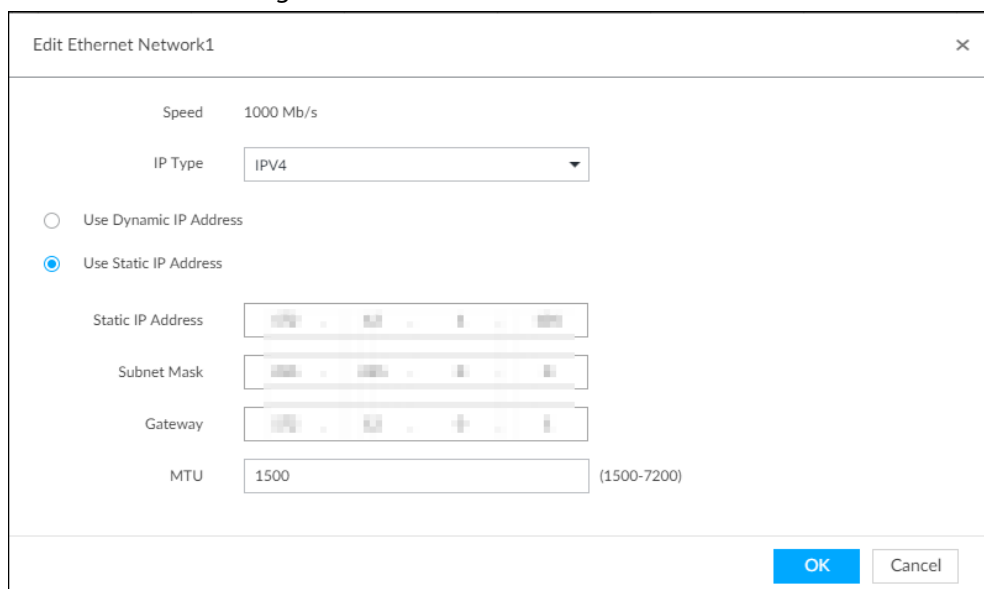
Click  to view the NIC parameter information.

Figure 6-2 TCP/IP




**Step 2** Click  of the corresponding NIC to edit network parameters.

Figure 6-3 Edit Ethernet network



**Step 3** Set parameters.

Table 6-1 TCP/IP parameters description

Parameters	Description
Speed	Current NIC max network transmission speed.
IP Type	Select IPv4 or IPv6.
Use Dynamic IP Address	When there is a DHCP server on the network, check the box to use dynamic IP address, system can allocate a dynamic IP address to the device. There is no need to set IP address manually.
Use Static IP Address	Check the box to use static IP address. Set static IP address, subnet mask and gateway. Set a static IP address for the device.
MTU	<p>Set NIC MTU value. The default setup is 1500 Byte.</p> <p>We recommend you to check the MTU value of the gateway first and then set the device MTU value equal to or smaller than the gateway value. It is to reduce the packets slightly and enhance network transmission efficiency.</p> <p> Changing MTU value might result in NIC reboot, network offline and affect current running operation. Please be careful!</p>

**Step 4** Click **OK**.

Go back to **TCP/IP** page.

**Step 5** Set DNS server information.

You can select to get DNS server manually or input DNS server information.



This step is compulsive if you want to use domain service.

- Check the box to auto get DNS server address, device can automatically get the DNS server IP address on the network.
- Check the box to use the following DNS server addresses, and then input primary DNS and alternate DNS IP address.

**Step 6** Set default NIC.

Select default NIC from the drop-down list.



Make sure that the default NIC is online.


**Step 7** Click **Save**.

### 6.2.1.2 Port Aggregation

Bind multiple NIC to create one logic NIC and use one IP address for peripheral device. The bonded NIC can work as the specified aggregation mode to work. It enhances network bandwidth and network reliability.



System supports configuring load balance, fault tolerance, and link aggregation.

Table 6-2 Aggregation mode description

Aggregation mode	Description
Load balance	<p>Device has bonded several NICs at the same time and use one IP address to communicate with the external device. The bonded NICs are working together to bear the network load.</p> <p>The load balance mode adds the network throughput data amount and enhances network flexibility and availability. In this mode, the network is offline once all NICs break down.</p>
Fault-tolerance	<p>In this mode, device has bonded several NICs and set one NIC as the main card and the rest NICs are the alternative NICs. Usually, only the main NIC card is working. System can automatically enable other alternate cards to work when the main card breaks down.</p> <p>Fault-tolerance is a network mode to enhance NIC reliability. In this mode, the network is offline once all NICs break down.</p>
Link aggregation	<p>Device has bonded several NICs and all NICs are working together to share the network load. System allocates data to each NIC according to your allocated strategy. Once the system detects that one NIC breaks down, it stops sending data with this NIC, and then system transmits the data among the rest NICs. System calculates transmission data again after malfunctioning NIC resumes work.</p> <p>In this mode, the network is offline once all bonded NICs are malfunctioning.</p> <p> Make sure that the switch supports link aggregation and you have set the link aggregation mode.</p>

### 6.2.1.2.1 Binding NIC

System supports load balance, fault-tolerance, and link aggregation. Select bind mode according to your actual requirements.

**Step 1** Click  or click  on the configuration page, and then select **NETWORK > Basic Network > TCP/IP**.

**Step 2** Bind NICs.

- 1) Click **Port Aggregation**.
- 2) Select the NICs you want to bind.
- 3) Select an aggregation mode.
- 4) Click **Port Aggregation**.

The corresponding setting page is displayed.




The setting page varies depending on the aggregation mode you have selected. The following figure is the load balance setting page.

Figure 6-4 Edit load balance

5) Set parameters.

Table 6-3 TCP/IP parameters description

Parameters	Description
Speed	Maximum network transmission speed of current NIC.
IP Type	Select IPv4 or IPv6.
Use Dynamic IP Address	When there is a DHCP server on the network, check the box to use dynamic IP address. System can allocate a dynamic IP address to the device. There is no need to set IP address manually.
Use Static IP Address	Check the box to use static IP address. Set static IP address, subnet mask and gateway. It is to set a static IP address for the device.
MTU	<p>Set NIC MTU value. The default setup is 1500 Byte.</p> <p>We recommend you to check the MTU value of the gateway first and then set the device MTU value equal to or smaller than the gateway value. It is to reduce the packets slightly and enhance network transmission efficiency.</p> <p></p> <p>Changing MTU value might result in NIC reboot, network offline and affect current running operation. Please be careful!</p>

6) Click **OK**.

Go back to **TCP/IP** page.

**Step 3** Click **Save**.

System pops up a confirmation box.



**Step 4** Click **OK**.

The binding card information becomes activated after reboot operation.



### 6.2.1.2.2 Cancelling Binding NIC

Cancel port aggregation and allow the bonded NICs to work as independent card.

**Step 1** Click  or click  on the configuration page, and then select **NETWORK > Basic Network > TCP/IP**.

**Step 2** Select a bonded NIC.

**Step 3** Click **OK**.  
System splits the bonded NIC.



After splitting NIC binding, the first NIC reserves the IP address configured during binding, while the rest NICs restore default IP addresses.

### 6.2.1.3 Setting Port Number

Set device port number.



**Step 1** Click  or click  on the configuration page, and then select **NETWORK > Basic Network > Port**.

Figure 6-5 Port

**Step 2** Set parameters.



Log in again after modifying parameters except **Max Connection**.

Table 6-4 Connection setting parameters description

Parameters	Description
Max Connection	The allowable maximum clients accessing the Device at the same time, such as web, PCAPP, and Platform. Select a value between 1 and 128. The default value setting is 20.
TCP Port	Set according to the actual requirements. The default value is 37777. The value ranges from 1025 to 65535.
RTSP Port	Set according to the actual requirements. The default value is 554. The value ranges from 1 to 65535.

Parameters	Description
HTTP Port	Set according to the actual requirements. The default value is 80. The value ranges from 1 to 65535. If the value you set is not 80, please add the port number after the IP address when you are using browser to login the device.
HTTPS Port	Set according to the actual requirements. The default value is 443. The value ranges from 1 to 65535.
UDP Port	Set according to the actual requirements. The default value is 37778. The value ranges from 1025 to 65535.

**Step 3** Click **Save**.

System reboots corresponding service of the port.

## 6.2.2 Network Apps

Set device network parameters, so that system can connect to other devices.

### 6.2.2.1 UPnP



Through the UPnP (Universal Plug and Play) protocol, you can establish a mapping relationship between the LAN and the WAN, the WAN user can use the WAN IP address to directly access the device in the LAN.



Device services and ports will be mapped to the public network after UPnP is enabled. Be cautious.








- Make sure that your PC has UPnP network services installed.
- Log in to the router and set the WAN port IP address of router.
- Enables the UPnP function on the router.
- Connect the device to the router LAN (Local Area Network, LAN) port.
- Select **NETWORK > Basic Network > TCP/IP**, and then set the IP address to be the private-network IP of the router, or select DHCP to automatically obtain the IP address.

**Step 1** Click  or click  on the configuration page, and then select **NETWORK > Network Apps > UPnP**.

**Step 2** Set parameters.

Table 6-5 Register

Parameters	Description
Port Mapping	Click  to enable UPnP.
LAN IP	The LAN IP address of router.  The IP address is automatically obtained after the mapping succeeds.
WAN IP	The WAN IP address of router.  The IP address is automatically obtained after the mapping succeeds.

Parameters	Description
Port Mapping List	<p>The list is consistent with the UPnP port mapping list on the router.</p> <ul style="list-style-type: none"> <li>• Internal Port: The EVS port to be mapped on the router.</li> <li>• External Port: The WAN port of the internal port.</li> </ul> <p></p> <ul style="list-style-type: none"> <li>• When setting the external port, use the ports between 1024 and 5000, and do not use the well-known ports 1 to 255 and the system ports 256 to 1023, so as to avoid conflicts.</li> <li>• When there are multiple devices within the LAN, properly plan the port mapping to avoid conflicts of WAN ports.</li> <li>• When making a port mapping, make sure that the port you are mapping is not occupied or restricted.</li> <li>• The TCP/UDP WAN and LAN ports must be consistent and cannot be modified.</li> </ul>
Modification	Click  , and then you can modify the external port.

**Step 3** Click **Save**.

Enter *http://WAN IP: WAN port number* in the browser to access the device with the corresponding port number in the router network.

## 6.2.2.2 Multicast

When multiple users are viewing live video of the same device at the same time, it might cause failure due to limited bandwidth. To solve this problem, you can set a multicast IP address (224.0.0.0–239.255.255.255) for the Device.



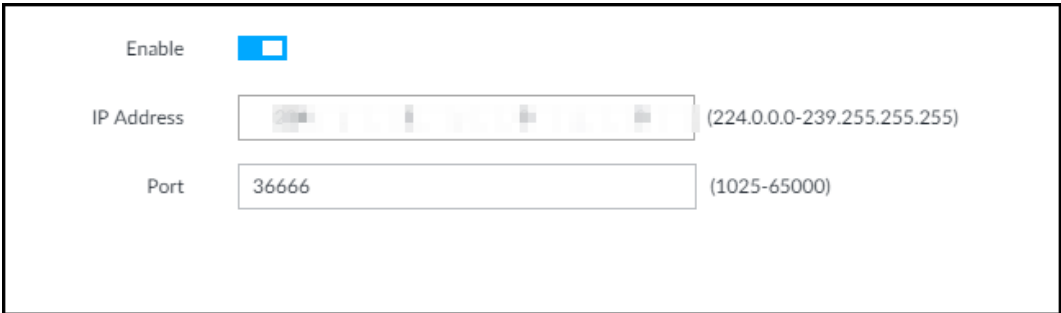
**Step 1** Click  or click  on the configuration page, and then select **NETWORK > Network Apps > Multicast**.

Figure 6-6 Multicast



**Step 2** Click  to enable multicast.

**Step 3** Set parameters.

Table 6-6 Parameters

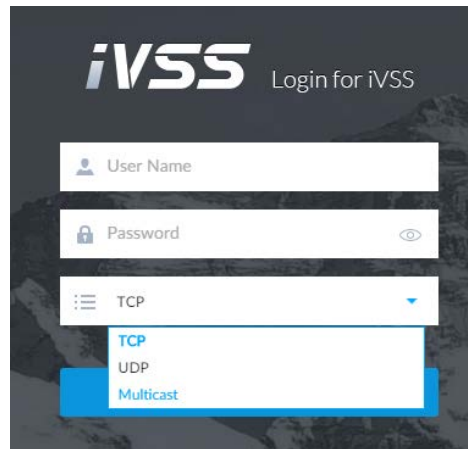
Parameters	Description
IP Address	Set the multicast IP address of the device (224.0.1.0–239.255.255.255).
Port	Set the multicast port (1025–65000).

**Step 4** Click **Save**.



After configuring the multicast address and port, you can log in to the web interface or PCAPP client through the multicast protocol.

Take PCAPP for example. On the login page of PCAPP, select **Multicast** as the login type. The PCAPP client will automatically obtain the multicast address and join the multicast group. After login, you can view live videos through multicast protocol.


Figure 6-7 Log in through multicast







## 6.3 Event Management

Click  or click  on the configuration page, select **EVENT**.

On the page, configure alarm event, including alarm event of iVSS and remote device.

- Select the root node  in the resource tree on the left to set alarm event of the Device.
- Select remote device in the device tree on the left, to set alarm event of this remote device.



- The alarm event might be different depending on the model you purchased.
-  means that the corresponding alarm event has been enabled.
-  means that AI by camera has been enabled;  means that AI by device has been enabled;  means that both have been enabled.


### 6.3.1 Alarm Actions

System can trigger the corresponding actions when an alarm occurs.



The supported actions might be different depending on the model you purchased.

On the alarm configuration page, click **Actions** to display actions. Configure actions according to your actual need.

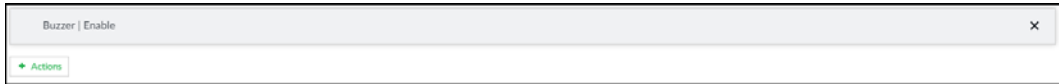
- After setting actions, click **Save** on the page.
- After enabling actions, click  to disable the corresponding actions.

#### 6.3.1.1 Buzzer

The system activates a buzzer alarm when there is corresponding alarm event.

Click **Actions** and select **Buzzer** to enable this function.

Figure 6-8 Buzzer

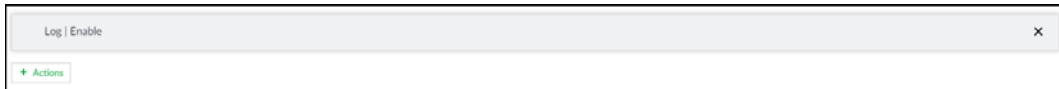


### 6.3.1.2 Log

Enable the log function. The system notes down the alarm information in the log when there is corresponding alarm event.

Click **Actions** and select **Log** to enable this function.

Figure 6-9 Log



When log function is enabled, after an alarm is triggered, click **+** on **LIVE** page, select **MAINTAIN > Log > Event**.

### 6.3.1.3 Email

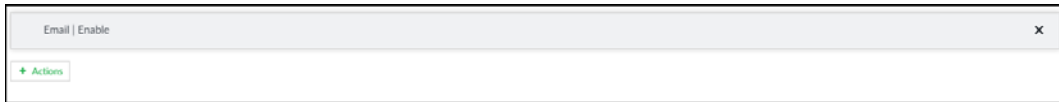
Enable Email function. The system sends alarm email to all added receivers when there is corresponding alarm event.



Make sure that the email configuration has been completed. See "6.3.1.3 Email" for detailed information.

Click **Actions** and select **Email** to enable this function.

Figure 6-10 Email



### 6.3.1.4 Local Alarm Out

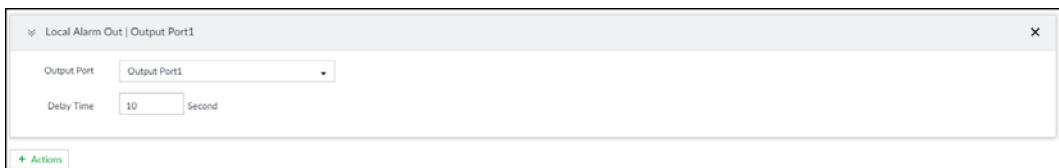
Set local alarm output. System can trigger the corresponding alarm event when an alarm occurs.



Make sure that IVSS is connected with alarm output device.

**Step 1** Click **Actions** and select **Local Alarm Out**.

Figure 6-11 Local alarm out



**Step 2** Select alarm output port.

You can select multiple alarm output ports.

**Step 3** Set delay time.

Set a delay time. After alarm event is ended, alarm will end after the delay time. You can configure from 0 seconds through 300 seconds, and the default value is 10 seconds.

### 6.3.1.5 Voice Prompt

Set voice prompt function. When there is an alarm, system can play the selected audio file.



Make sure that the voice function has been configured.

**Step 1** Click **Actions** and select **Voice Prompt**.

Figure 6-12 Voice prompt

**Step 2** In the **File Name** list, select the audio file that you want to play for this configured period.

**Step 3** Set delay time.

- **Play times:** Select **Play Times** and enter the times to play the file. After the alarm event is ended, system will continue to play the voice file according to the play times.
- **Duration:** Select **Duration** and enter the delayed play duration. After the alarm event is ended, system will continue to play the voice file according to the duration.

## 6.3.2 Local Device


Set IVSS alarm event, including abnormal event, device offline alarm, AI plan, and local device alarm.


### 6.3.2.1 Abnormal Event

Set the alarm mode when an abnormal event occurs.



The Device supports HDD, storage error, network, AI module, fan and power fault alarm.

Table 6-7 Abnormal event description

Name	Description
No HDD	System triggers an alarm when there is no HDD. It is enabled by default.
Storage error	System triggers an alarm in case of HDD error, RAID degrade, RAID broken, and storage pool error. It is enabled by default.
Storage space full	System triggers an alarm when the used storage space reaches the pre-defined threshold. It is disabled by default.  The alarm is valid only when the storage mode is set as <b>Stop</b> on the <b>Local Hard Disk</b> page. For details, see "6.4.1.4 Setting Storage Strategy".
IP conflict	System triggers an alarm when its IP address conflicts with IP address of other device in the same LAN. It is enabled by default.
MAC conflict	System triggers an alarm when its MAC address conflicts with MAC address of other device in the same LAN. It is enabled by default.

Name	Description
Lock in	System triggers an alarm when an account login error has reached the threshold. At the same time, system locks current account. It is disabled by default.  Go to the <b>Security</b> page to set account error threshold. See "6.6.3 Safety Protection" for detailed information.
AI module temp	When AI module temperature is higher than the specified value, system triggers an alarm. It is enabled by default.
AI module offline	When AI module and system is disconnected, system triggers an alarm. It is enabled by default.
Fan speed alarm	When IVSS fan speed is abnormal, system triggers an alarm. It is enabled by default.
Power fault	When IVSS power supply is abnormal, system triggers an alarm. It is disabled by default.

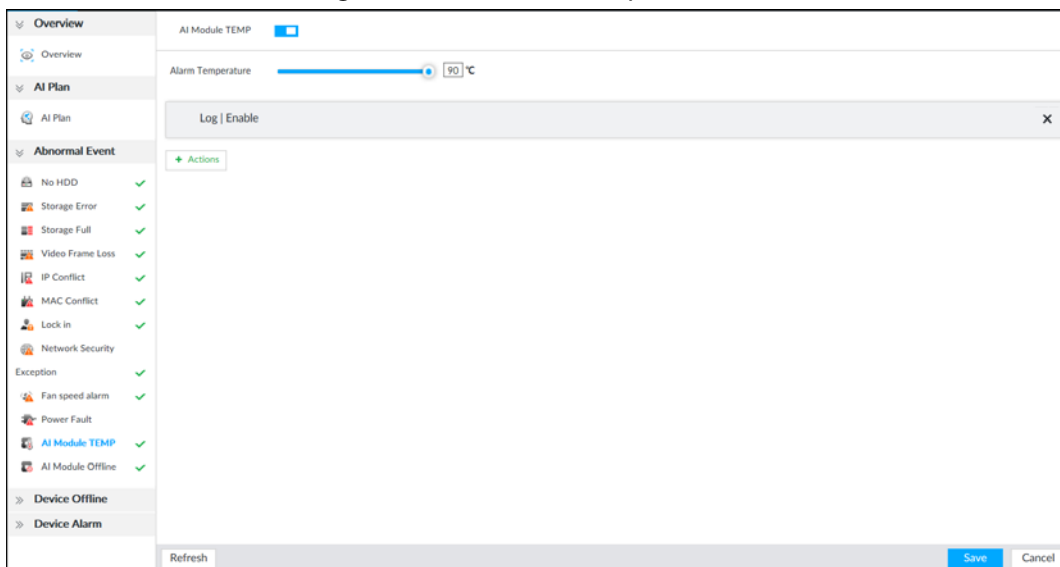
Here we use AI module temp for example. For other events, the setting steps are similar. See the actual page for detailed information.


**Step 1** Click  or click  on the configuration page, and then select **EVENT**.

**Step 2** Select the root node in the device tree.

**Step 3** Select **Abnormal Event** > **AI Module TEMP**.

Figure 6-13 AI module temp



**Step 4** Click  to enable AI module temperature alarm function.

**Step 5** Drag  to set alarm temperature threshold.



The above step is for AI module temperature alarm only.

**Step 6** Click **Actions** to set alarm actions. See "6.3.1 Alarm Actions" for detailed information.

**Step 7** Click **Save**.

### 6.3.2.2 Configuring AI Module Slot Number

Configure the number of AI modules designated to task scheduling.



- Step 1** Click  or click  on the configuration page, and then select **EVENT**. The **EVENT** page is displayed.
- Step 2** Select a camera in the device tree on the left.
- Step 3** Select **AI Plan > AI Plan > AI Module slot number**.
- Step 4** Configure the parameters.

Figure 6-14 AI module slot number



Table 6-8 AI module slot number parameters



Parameter	Description
Task scheduling– picture stream	Configure the number of AI modules allocated to picture stream for task scheduling. The value is 50 percent of the actual number of AI modules by default.
Task scheduling– video stream	Configure the number of AI modules allocated to video stream for task scheduling. The value is 50 percent of the actual number of AI modules by default.



If the total number of AI modules configured does not equal to the actual number of AI modules, the system will prompt you to reset.

- Step 5** Click **Save**.

## 6.4 Storage Management

Click  or click  on the configuration page, select **STORAGE**. The **Local Hard Disk** page is displayed. Manage storage resources (such as recording file) and space, so you can use and improve utilization ratio of storage space.



The system supports pre-check and routine inspection, and displays health status, so you can obtain real-time status of device and avoid data loss.



- **Pre-check:** During device operation, the system automatically detects disc status in case of change (reboot, insert and pull the disc).






- Routine inspection: the system carries out routine inspection of the disc continuously. During device operation, the disc might go wrong due to service life, environment and other factors. Find out any problems during routine inspection.

## 6.4.1 Local Hard Disk

The local hard disk refers to the HDD installed on the system. On this page, you can view HDD space (free space/total space), temperature (centigrade/Fahrenheit), HDD information and so on.

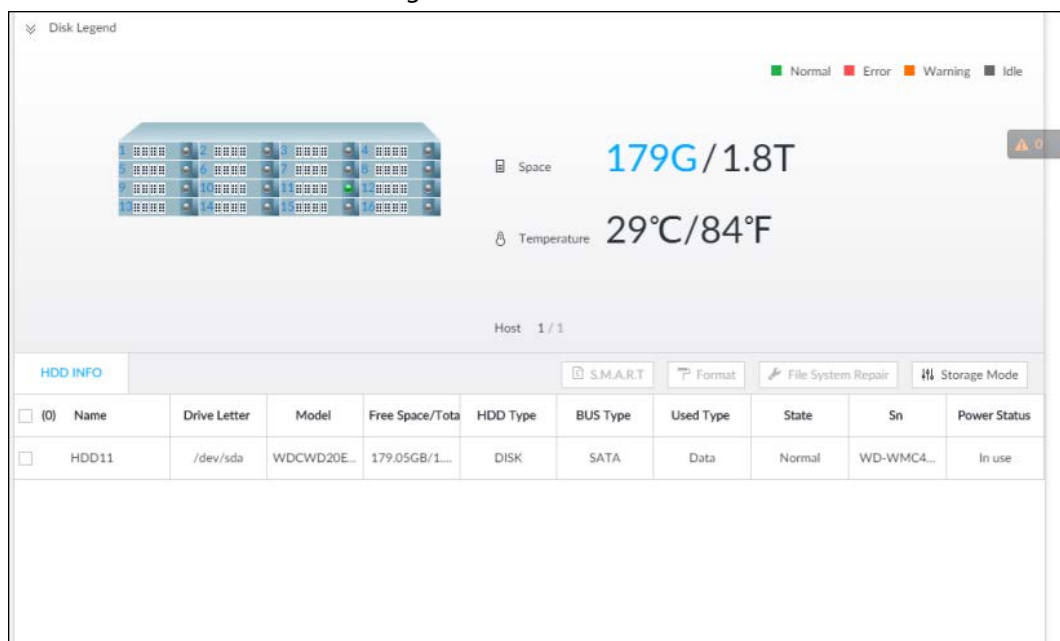
Click  or click  on the configuration page, and then select **STORAGE > Storage Resource > Local Hard Disk**. There is a corresponding icon near the HDD name after you create the RAID and hot spare HDD.

- : RAID HDD.
- : Global hot spare HDD.
- : Invalid HDD of RAID group.



Slight difference might be found on the user interface.

Figure 6-15 HDD



### 6.4.1.1 Viewing S.M.A.R.T

S.M.A.R.T is Self-Monitoring Analysis and Reporting Technology. It is a technical standard to check HDD drive status and report potential problems. System monitors the HDD running status and compares with the specified safety value. Once the monitor status is higher than the specified value, system displays alarm information to guarantee HDD data security.



Check one HDD to view S.M.A.R.T information at one time.

On the **Local Hard Disk** page, select a HDD, and then click **S.M.A.R.T**. The **S.M.A.R.T** page is displayed. Check whether the HDD status is **OK** or not. If there is any problem, fix it in time.

Figure 6-16 S.M.A.R.T

Sn	Note	Value	Worst	Boundary	Original Data	State
1	Read Error Rate	117	99	6	135185072	Better
3	Spin Up Time	97	97	0	0	Better
4	Start/Stop Co...	100	100	20	780	Better
5	Reallocated S...	100	100	36	0	Better
7	Seek Error Rate	67	60	30	17203264542	Better
9	Power On Ho...	98	98	0	2426	Better
10	Spin-up Retry...	100	100	97	0	Better
12	Power On/Of...	100	100	20	752	Better
184	End-to-End F...	100	100	99	0	Better

### 6.4.1.2 Format



- Formatting HDD will clear all data on the HDD. Be careful!
- Hot spare HDD cannot be formatted.

Enter the **Local Hard Disk** page, select one or more HDD(s), and click **Format**. It is to format the selected HDD.

### 6.4.1.3 File System Repair

Once you cannot mount the HDD or you cannot properly use the HDD, you can try to use the **File System Repair** function to fix the problem.

Enter the **Local Hard Disk** page, select one or more HDD(s) you cannot mount, and click **File System Repair**, you can repair the selected file system of the corresponding HDD(s). The repaired HDD can work properly or to be mounted.

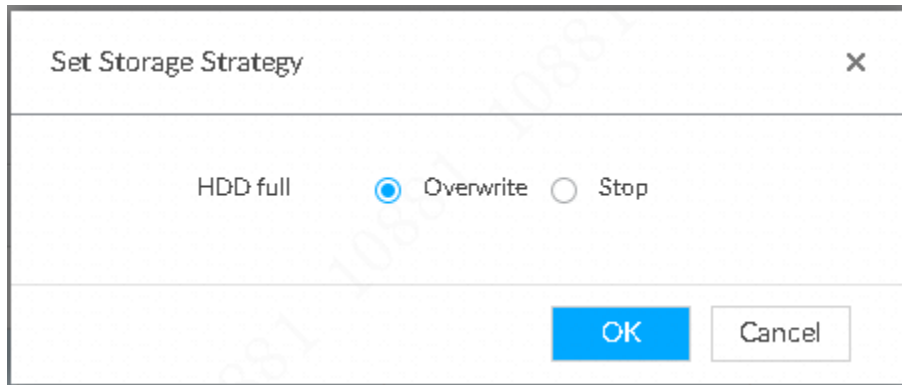
### 6.4.1.4 Setting Storage Strategy

Set storage strategy when HDD space is full.

**Step 1** Click or click on the configuration page, and then select **STORAGE > Storage Resource > Local Hard Disk**.

**Step 2** Click **Storage Mode**.

Figure 6-17 Set storage strategy



**Step 3** Set storage mode.

- **Overwrite:** When HDD free space is less than 150 G or 4% of the total space (the larger of the two values prevails), system continues to record and begins overwriting the earliest record file.
- **Stop:** When HDD free space is less than 150 G or 4% of the total space (the larger of the two values prevails), system stops recording. Stop recording will trigger an alarm. For details, see "6.3.2.1 Abnormal Event".

**Step 4** Click **OK** to save the configuration.

### 6.4.1.5 Viewing RAID Group

Click or click on the configuration page, and then select **STORAGE > Storage Resource > Local Hard Disk > RAID Group**. You can view free space, RAID type, working mode and status of RAID group.

Figure 6-18 RAID group

HDD INFO		RAID Group			
Name	Free Space/Total	RAID Type	Working Mode	State	
RAID_1	10 P1TB/10 P1TB	RAID0	--	Active	

Total 1 Item(s) Show up to 100

Refresh

- Click next to the RAID name to display the RAID member list, and then you can view RAID member details.
- Point to the **Status** column, and then click to display the **Details** page to view RAID group details.

## 6.4.2 RAID

RAID (Redundant Array of Independent Disks) is a data storage virtualization technology that combines multiple physical HDD components into a single logical unit for the purposes of data redundancy, performance improvement, or both.



- The Device supports RAID0, RAID1, RAID5, RAID6, RAID10, RAID50 and RAID60. See "Appendix 2 RAID" for detailed information.
- You are recommended to use enterprise HDD when you are creating RAID, and use surveillance HDD for single-HDD mode.

## 6.4.2.1 Creating RAID

RAID has different levels such as RAID5, RAID6 and so on. Different RAID levels have different data protection, data availability and performance levels. Create RAID according to your actual requirements.



Creating RAID operation is going to clear all data on these HDD. Be careful!

### 6.4.2.1.1 Creating RAID



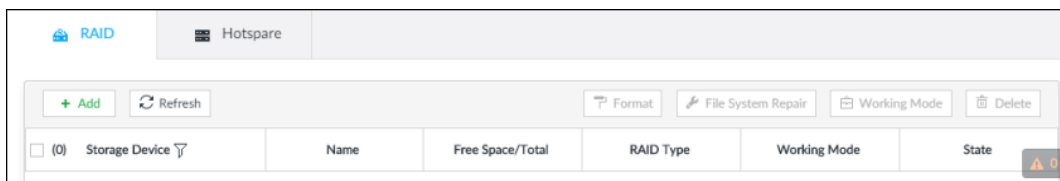
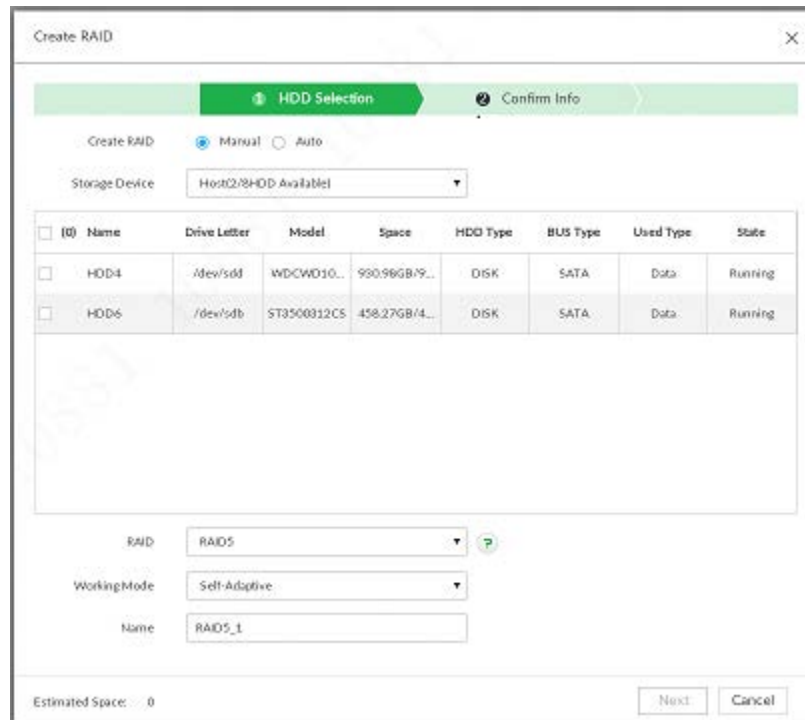
**Step 1** Click , or click  on the configuration page, and then select **STORAGE > Storage Resource > RAID > RAID**.

Figure 6-19 RAID (1)



**Step 2** Click **Add**.

Figure 6-20 Create RAID (1)




**Step 3** Set RAID parameters.  
Select RAID creation type according to actual situation. It includes **Manual RAID** and **Auto RAID**.

**Manual RAID:** System creates a specified RAID type according to the selected HDD amount.

- 1) Select **Manual RAID**.
- 2) Select HDD you want to use.
- 3) Set parameters.

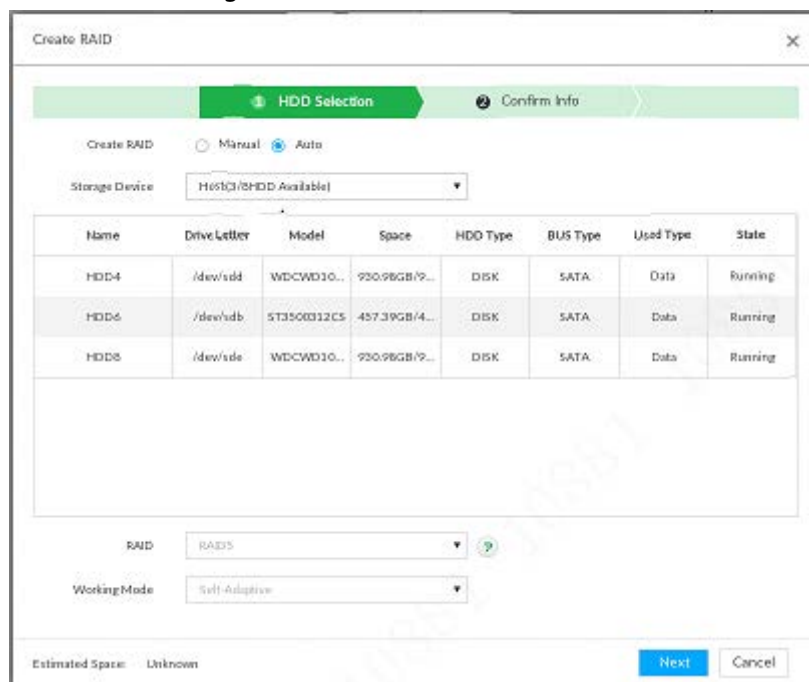
Table 6-9 Manual creation parameters description

Parameters	Description
Storage Device	Select storage device of the HDD and select the HDD you want to add to the RAID.  Different RAID types need different HDD amounts.
RAID	Select a RAID type you want to create.
Working mode	Set RAID resources allocation mode. The default setup is self-adaptive. <ul style="list-style-type: none"> <li>• Self-adaptive means the system can automatically adjust RAID synchronization speed according to current business load. When there is no external business, the synchronization speed is at high speed. When there is external business, the synchronization speed is at low speed.</li> <li>• Sync first: Allocate resources to RAID synchronization first.</li> <li>• Business first: Allocate resources to business first.</li> <li>• Load-Balance: Allocate resources to business and RAID synchronization equally.</li> </ul>
Name	Set RAID name.

**Auto:** System creates RAID5 according to the HDD amount.

- 1) Select **Auto**.

Figure 6-21 Create RAID (2)



- 2) Set parameters.

Table 6-10 Auto parameters description

Parameters	Description
Storage Device	Select storage device of the HDD.
Working mode	<p>Set RAID resources allocation mode. The default setup is self-adaptive.</p> <ul style="list-style-type: none"> <li>Self-adaptive means the system can automatically adjust RAID synchronization speed according to current business load. When there is no external business, the synchronization speed is at high speed. When there is external business, the synchronization speed is at low speed.</li> <li>Sync first: Allocate resources to RAID synchronization first.</li> <li>Business first: Allocate resources to business first.</li> <li>Load-Balance: Allocate resources to business and RAID synchronization equally.</li> </ul>

Step 4 Click **Next**.

Figure 6-22 Confirm info (manual)

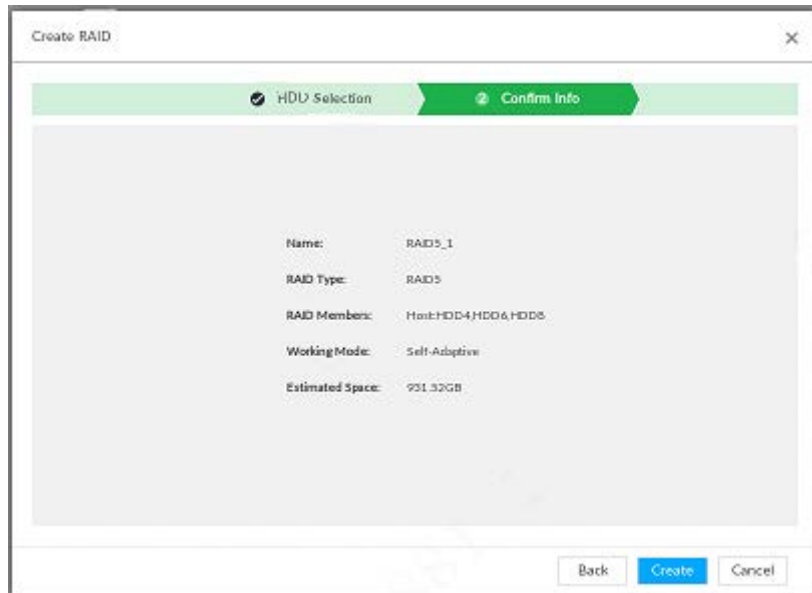
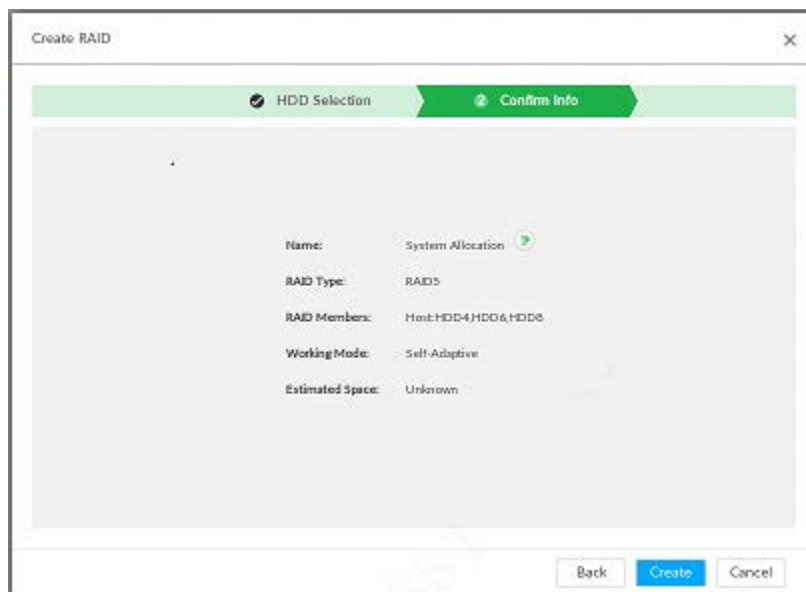


Figure 6-23 Confirm info (Auto)



**Step 5** Confirm info.

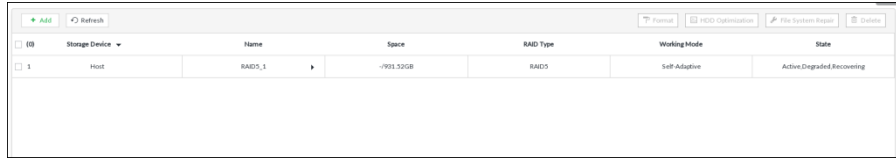


If the input information is wrong, click **Back** to set RAID parameters again.

**Step 6** Click **Create**.

System begins to create RAID. It displays RAID information after creation.

Figure 6-24 RAID (2)



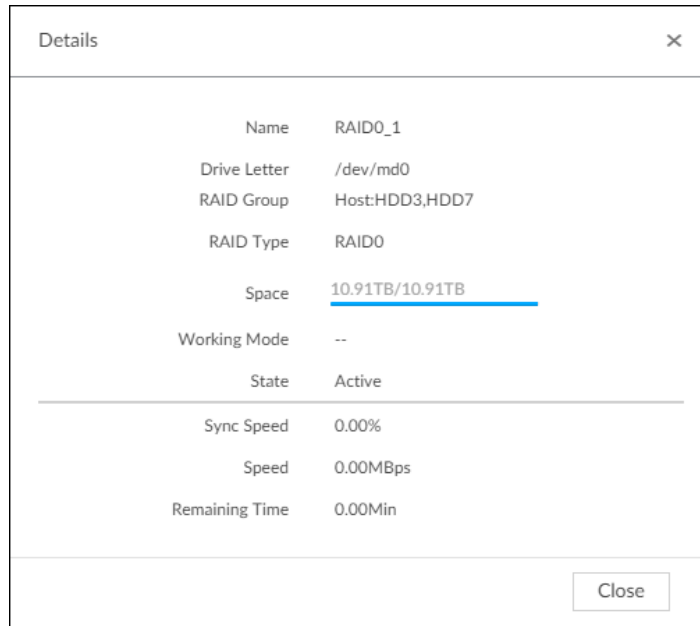
### 6.4.2.1.2 Operation

After creating RAID, view RAID disk status and details, clear up RAID, and repair file system.

Table 6-11 RAID operation

Name	Operation
View RAID HDD status	Click  at the right side of the RAID name to open the RAID HDD list. It is to view RAID HDD space, status and so on.
View RAID details	Click  to view RAID detailed information.
File System Repair	Once you cannot mount the RAID or you cannot properly use the RAID, you can try to use repair file system function to fix. Enter RAID page, select one or more RAID(s) you cannot mount, click <b>File System Repair</b> , you can repair the selected file system of the corresponding RAID(s). The repaired RAID can work properly or to be mounted.
Modify Working Mode	Select one or more RAID(s), and then click <b>Working Mode</b> to modify the working mode.
Format RAID	Enter RAID page, select one and more RAID groups. Click <b>Format</b> to format the selected RAID.  Formatting RAID is to clear all data on the RAID and cancel the RAID group. Please be careful.
Delete RAID	Enter RAID page, select one and more RAID groups. Click <b>Delete</b> to delete the selected RAID.  Deleting RAID is to clear all data on the RAID and cancel the RAID group. Please be careful.

Figure 6-25 RAID details



### 6.4.2.2 Creating Hot Spare HDD

When a HDD of the RAID group is malfunctioning or has a problem, the hot spare HDD can replace the malfunctioning HDD. There is no risk of data loss and it can guarantee storage system reliability.



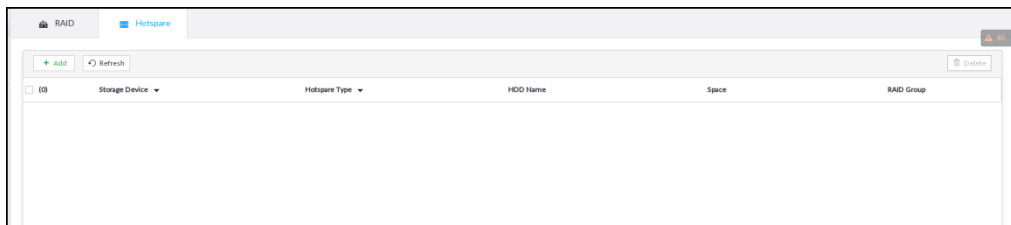
**Step 1** Click  or click  on the configuration page, and then select **STORAGE > RAID > Hot spare**.

Figure 6-26 Hot spare (1)



**Step 2** Click **Add**.

Figure 6-27 Global hot spare

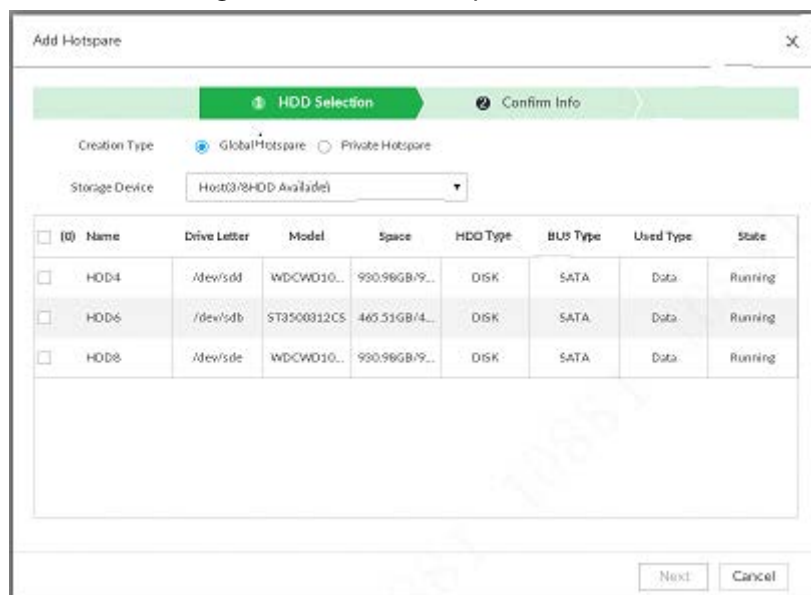
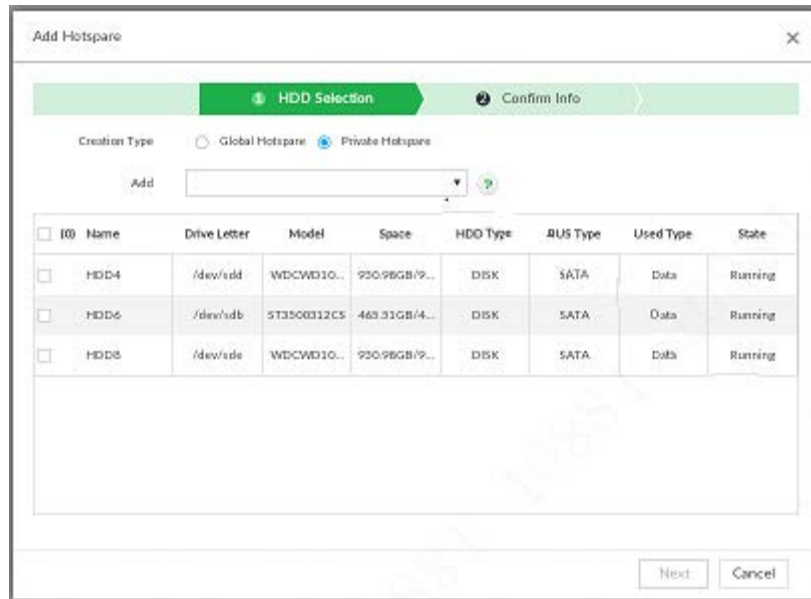




Figure 6-28 Private hot spare

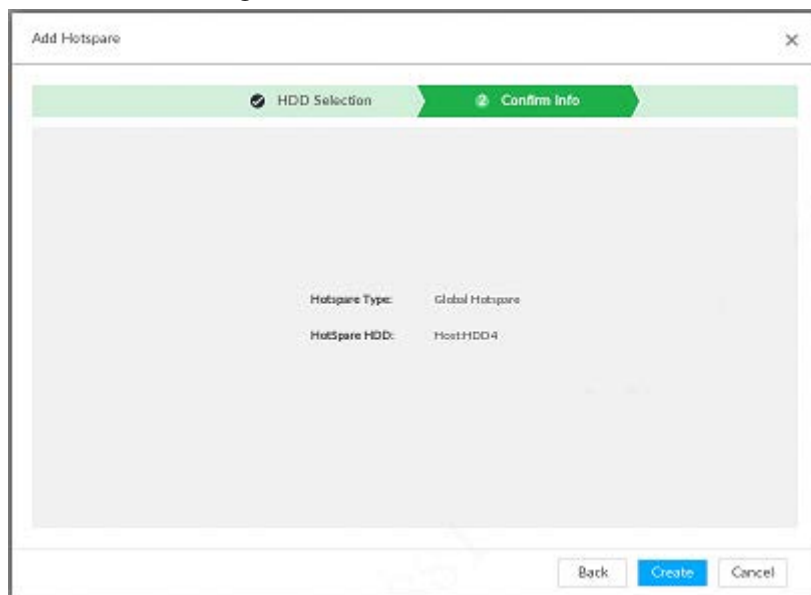


**Step 3** Select hot spare creation type.

- Global hot spare: Create hot spare for all RAID. It is not a hot spare HDD for a specified RAID group.
- Private hot spare: Select **Private Hot spare** and **Add** it to a RAID group. The private hot spare HDD is for a specified RAID group.

**Step 4** Select one or more HDD(s) and then click **Next**.

Figure 6-29 Confirm info



**Step 5** Confirm info.

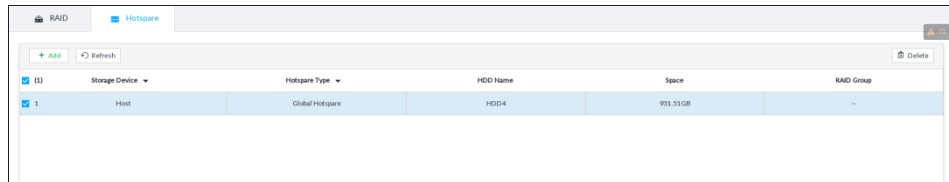


Click **Back** to select hot spare HDD(s) again if you want to change settings.

**Step 6** Click **Create** to save settings.

System displays the added hot spare HDD information.

Figure 6-30 Hot spare (2)



Select a hot spare HDD and then click **Delete**, it is to delete hot spare HDD.

## 6.4.3 Network Hard Disk

Network hard disk is a network-based online storage service that stores device information in the network hard disk through the iSCSI protocol.

### 6.4.3.1 iSCSI Application

View network hard disk usage, including remaining capacity, and hard disk status.



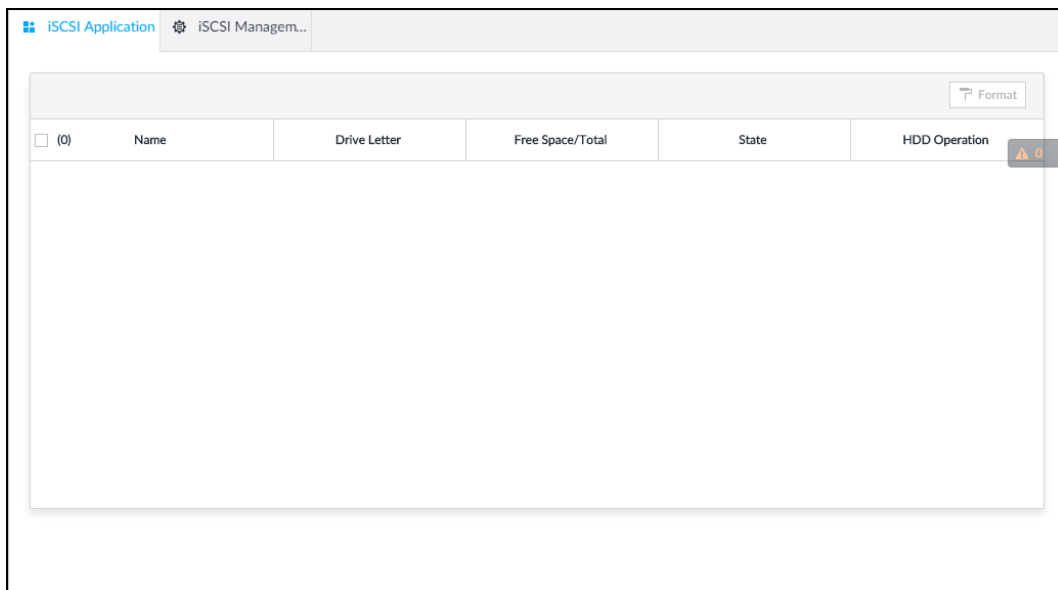
Click  or click  on the configuration page, and then select **STORAGE > Storage Resource > Network Hard Disk > iSCSI Application**.

Figure 6-31 iSCSI application



- Select a network hard disk, and then click **Format** to format the disk. Formatting your hard disk will erase all data from your hard disk, so do it carefully.
- Click the **HDD Operation** column, and then you can select an HDD operation permission type.
  - ◇ Read/Write: One can read, edit, add, and delete data of this disk.
  - ◇ Read Only: One can only read data of this disk.

### 6.4.3.2 iSCSI Management

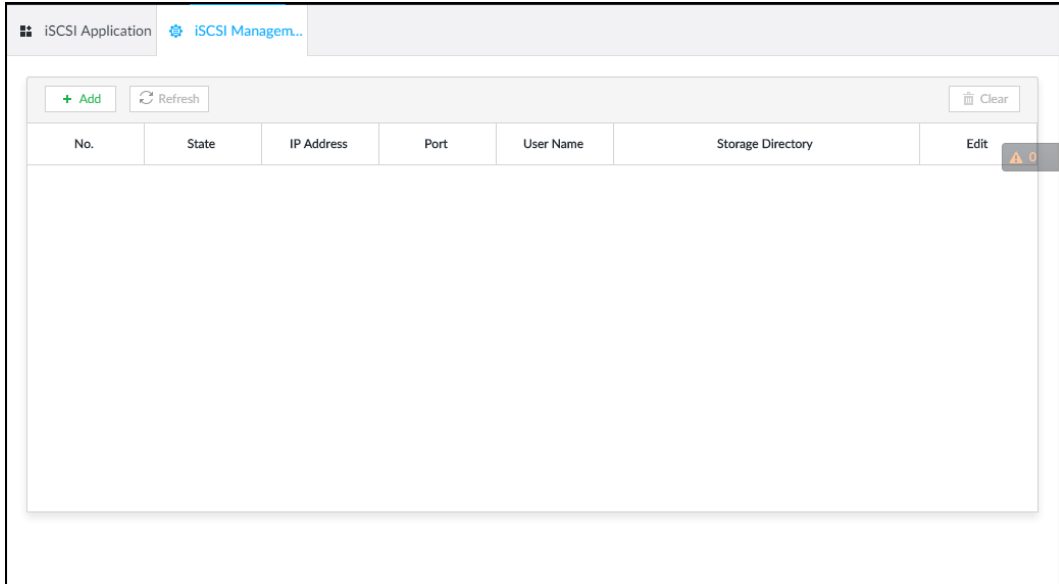
Set up the network disk through iSCSI and map the network disk to the device so that the device can use the network disk for storage.



Make sure that service has been enabled on the iSCSI server and the server has provided the shared file directory.

**Step 1** Click or click on the configuration page, and then select **STORAGE > Network Hard Disk > iSCSI Management**.

Figure 6-32 Network hard disk






**Step 2** Click .

Figure 6-33 Add iSCSI

**Step 3** Set parameters.

Table 6-12 Network hard disk parameters


Parameters	Description
Server IP	Enter iSCSI server IP address.

Parameters	Description
Port	Enter iSCSI server port number. It is 3260 by default.
Anonymous	<p>If iSCSI server has no permission limitation, you can select anonymous login.</p> <ul style="list-style-type: none"> <li>•  indicates that anonymous login is enabled and there is no need to set username and password.</li> <li>•  indicates that anonymous login is disabled.</li> </ul>
Username	If access permission has been limited when creating the shared file directory on the iSCSI server, you need to enter username and password.
Password	
Storage Directory	<p>Click <b>Search Directory</b> to select the storage directory.</p>  <p>The storage directory is generated when the shared file directory is being created on the iSCSI server. Each directory is an iSCSI disk.</p>

**Step 4** Click **OK**.

The added network disk is displayed.





- Click  to delete a disk; click **Refresh** to refresh the disk list.
- On the Disk Group page, you can configure network disk groups.





## 6.5 Video Recording

Disk and created RAID group are allocated to group 1 by default. You can allocate disk and RAID group to other groups according to your actual needs.

The default number of disk group is the same as the maximum number of HDD that IVSS supports. For example, the Device supports a maximum number of 16 HDDs, and then the default number of disk group is 16.

**Step 1** Click , or click  on the configuration page, and then select **VIDEO RECORDING > Storage Mode > Disk Group**.



- The value (such as ) next to the group name refers to the number of HDD and RAID group in the disk group. If instead,  is displayed, it means no available HDD or RAID group in the disk group, but there is video or image stored in the disk group.
-  indicates picture storage.  indicates video storage

**Step 2** Click a disk group.

**Step 3** Select HDD or RAID group from **Disks**, and then drag the HDD or the RAID group to another disk group.

Disk grouping takes effect immediately.



Select **All** to select all the HDDs and RAID groups of the disk group.

After configuring disk groups, you can also view which disk group the selected disk, video or picture belongs to.

## 6.6 Security Strategy



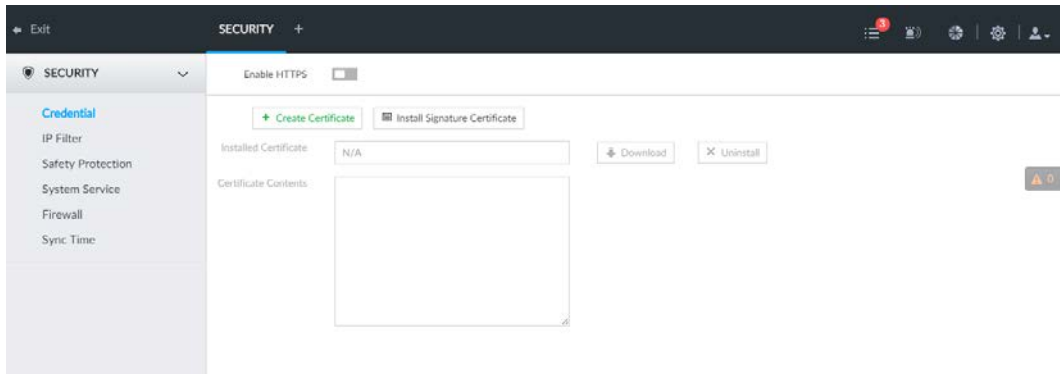
Click  or click  on the configuration page, select **SECURITY**. The **SECURITY** page is displayed. Set security strategy to guarantee device network and data safety. It includes HTTPS, set host IP access rights, enable network security protection.

Figure 6-34 Security center



### 6.6.1 HTTPS

HTTPS can use the reliable and stable technological means to guarantee user information and device security and communication data security. After installing the certificate, you can use the HTTPS on the PC to access the device.



- HTTPS function is for web interface and PCAPP only.
- You are recommended to enable HTTPS service. Otherwise, you might risk data leakage.

#### 6.6.1.1 Installing Certificate

There are two ways to install the certificate.

- Manually create a certificate and then install.
- Upload a signature certificate and then install.

##### 6.6.1.1.1 Installing the Created Certificate

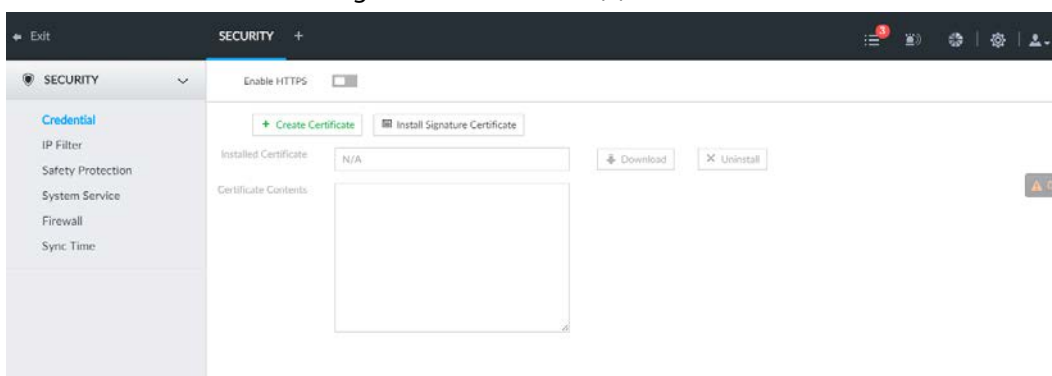
Install the created certificate manually. It includes creating the certificate on the device, downloading and installing the certificate on the PC.



- Create and install root certificate if it is your first time to use HTTPS or you have changed device IP address.
- After creating server certificate and installing root certificate, download and install root certificate on the new PC, or download the certificate and then copy to the new PC.

Step 1 Click  or click  on the configuration page, and then select **SECURITY > Credential**.

Figure 6-35 Credential (1)



**Step 2** Create certificate on the device.

- 1) Click **Create certificate**.
- 2) Set parameters as required.



IP/domain shall be the device IP or the domain.

- 3) Click **OK**.

System begins to install certificate, and then displays certificate information after the installation.

**Step 3** Download certificate.

- 1) Click .

The **Opening ca.crt** page is displayed.

- 2) Click **Save File** to select file saved path.
- 3) Click **Save**.

System begins downloading certificate file.

**Step 4** Install root certificate on the PC.

- 1) Double-click the certificate.

System displays **Open file-security warning** page.

- 2) Click **Open**.
- 3) Click **Install Certificate**.
- 4) Follow the prompts to import the certificate.

System goes back to **Certificate** page.

**Step 5** Click **OK** to complete certificate installation.

### 6.6.1.1.2 Installing Signature Certificate

Upload signature certificate to install.

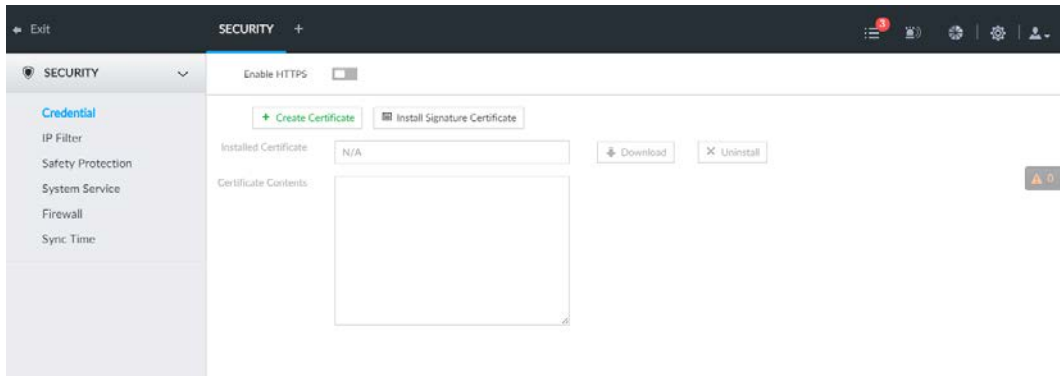
#### Preparation

Before installation, make sure that you have obtained safe and valid signature certificate.

#### Operation Steps

**Step 1** Click  or click  on the configuration page, and then select **SECURITY > Credential**.

Figure 6-36 Credential(1)



**Step 2** Click **InstallSignatureCertificate**.

**Step 3** Click **Browse** and then select certificate and credential file.

**Step 4** Click **Install**.

System begins to install certificate, and then displays certificate information after the installation.

**Step 5** Install the root certificate on the PC. See "6.6.1.1.1 Installing the Created Certificate" for detailed information.



This root certificate is the one obtained with signed certificate.

## 6.6.1.2 Enabling HTTPS

After you install the certificate and enable HTTPS function, you can use the HTTPS on the PC to access the device.

**Step 1** Click  or click  on the configuration page, and then select **SECURITY** > **Credential**.


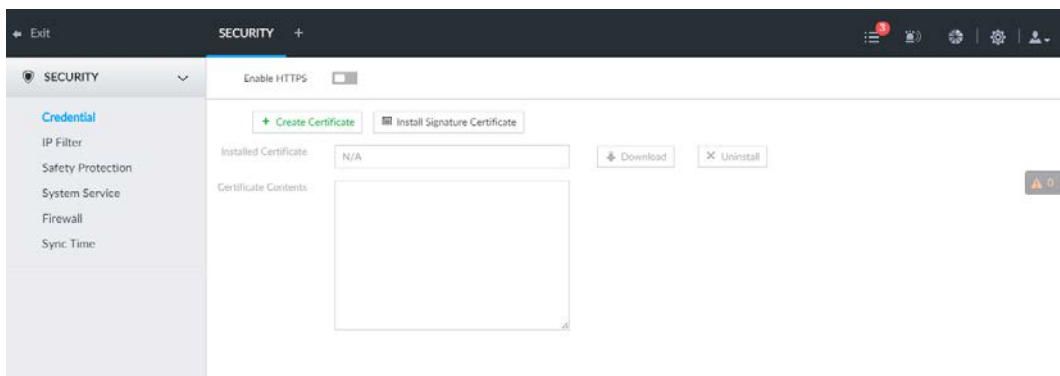
**Step 2** Click  to enable HTTPS function.

Figure 6-37 Credential



**Step 3** Click **Save**.

After you successfully save the settings, you can use HTTPS to access the web interface. Open the browser, enter `https://IP address:port` in the address bar, and then press Enter, and the login page is displayed.



- IP address is device IP or the domain name.
- Port refers to device HTTPS port number. If the HTTPS port is the default value 443, just use `https://IP address` to access.

### 6.6.1.3 Uninstalling the Certificate

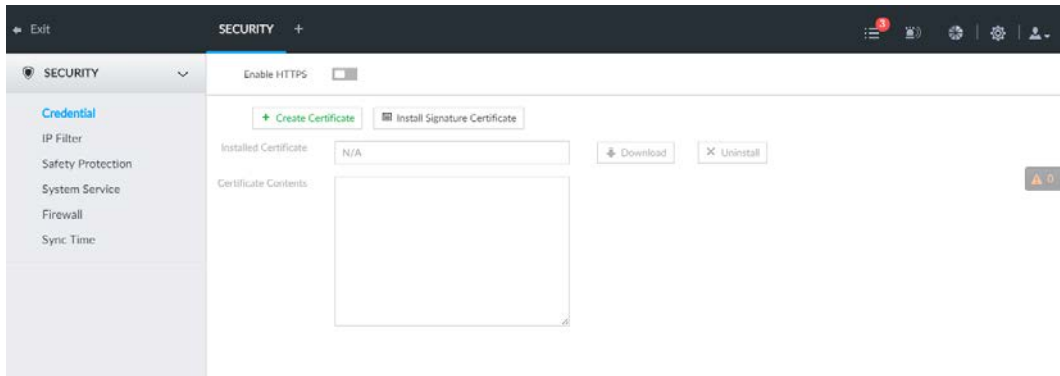
Uninstall the certificate.



- You cannot use the HTTPS function after you uninstall the certificate.
- The certificate cannot be restored after being uninstalled. Be cautious.

**Step 1** Click , or click  on the configuration page, and then select **SECURITY > Credential**.

Figure 6-38 Credential



**Step 2** Click **Uninstall**.

System pops up a confirmation box.

**Step 3** Click **OK** to uninstall the certificate.

### 6.6.2 Configuring Access Permission

Set the specified IP addresses to access the device, to enhance device network and data security.



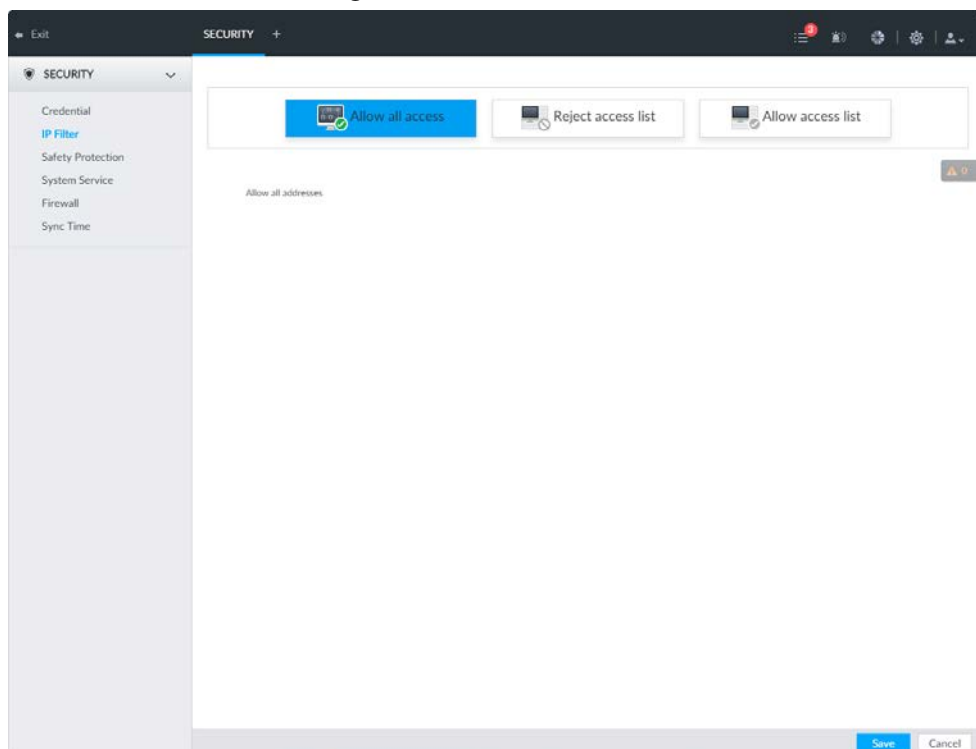
**Step 1** Click , or click  on the configuration page, and then select **SECURITY > IP Filter**.

Figure 6-39 IP Filter



**Step 2** Select IP access rights.



- Allow all access: It is to allow all IP addresses in the same IP segment to access the device.
- Reject access list: It means the IP address in the list cannot access the device.
- Allow access list: It means the IP address in the list can access the device.


Step 3 Add IP host.



The following steps are to set reject access list or allow access list.

- 1) Click **Add**.
- 2) Select **Add Type**, and set IP address or MAC address of IP host.
  - Single IP: Enter host IP address.
  - IP segment: Enter IP segment. It can add multiple IP addresses in current IP segment.
  - MAC: Enter MAC address of IP host.
- 3) Click **OK** to add the IP host.  
System displays added IP host list.



- Click **Add** to add more IP hosts.
- Click  to edit the IP host.
- Select an IP host and then click **Delete** to delete.

Step 4 Click **Save**.

## 6.6.3 Safety Protection

Set the login password lock strategy once the login password error has exceeded the specified threshold. System can lock current IP host for a period of time.



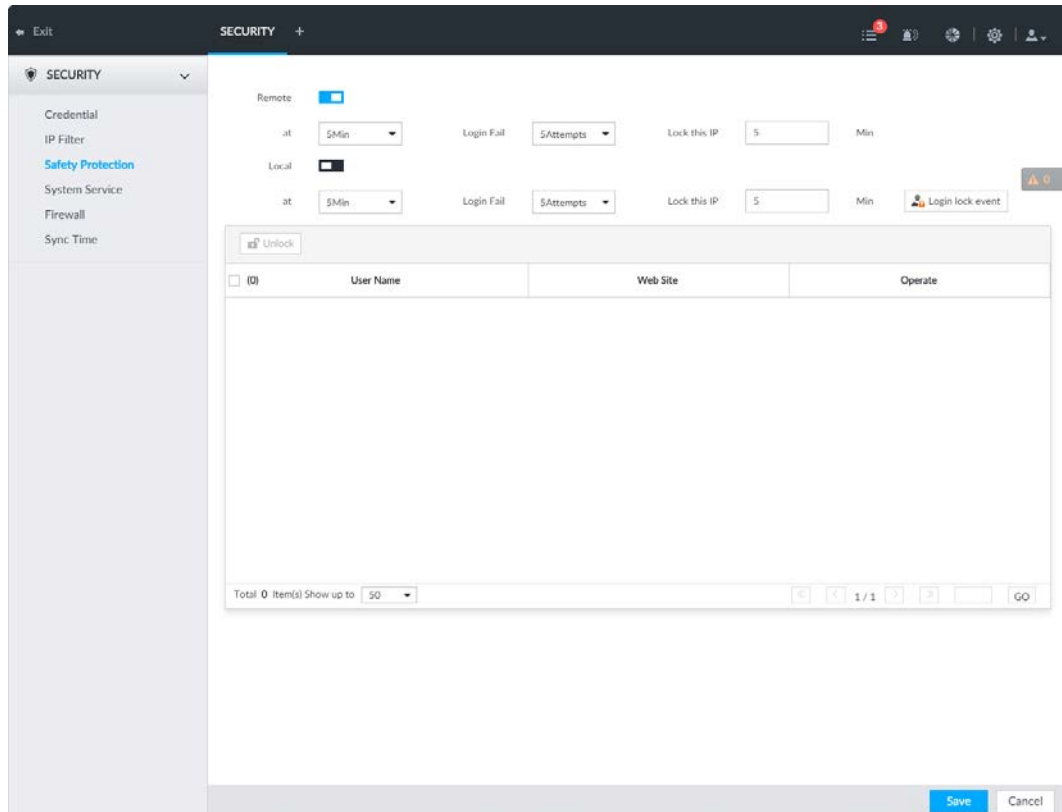

Step 1 Click  or click  on the configuration page, and then select **SECURITY > Safety Protection**.

Figure 6-40 Safety protection (1)



- Step 2** Click  to enable security protection function.
- Remote: When you are using web interface, PCAPP to access the device remotely, once the login password error has exceeded the threshold, system locks the IP host for a period of time.
  - Local: When you are accessing local menu of the device, once the login password error has exceeded the threshold, system locks the account for a period of time.
- Step 3** Set lock strategy according to the actual situation.
- Step 4** Click **Save**.  
Once the IP host has been locked, you can view the locked IP host on the list. Select an IP host and then click **Unlock**, or click the  of the corresponding IP host to unlock.
- Step 5** (Optional) Click **Login lock event** to go to the **Event** interface where you can select **Abnormal Event > Lock in** to configure a **Lock in** event.

## 6.6.4 Enabling System Service Manually

Enable system services for third-party access.



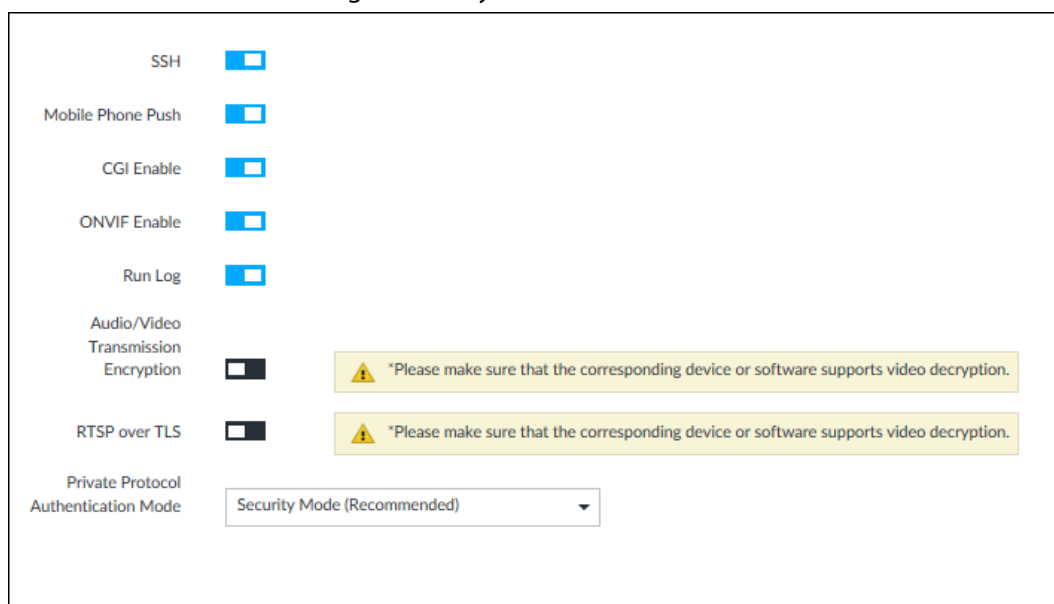




- Step 1** Click  or click  on the configuration page, and then select **SECURITY > System Service**.


Figure 6-41 System service



**Step 2** Enable or disable system service according to your actual situation.

Table 6-13 System service

System service	Description
SSH	<p>After enabling this function, you can access IVSS through SSH protocol to carry out system debugging and IP configuration. This function is disabled by default.</p> <p> You are recommended to disable this function. Otherwise there might be security risks.</p>
Mobile Phone Push	<p>After enabling this function, you can access IVSS with mobile phone client to receive information from IVSS.</p> <p> You are recommended to disable this function. Otherwise there might be security risks.</p>
CGI Enable	<p>After this function is enabled, third-party platform can connect IVSS through CGI protocol.</p> <p> You are recommended to disable this function. Otherwise there might be security risks.</p>
ONVIF Enable	<p>After this function is enabled, other devices can connect IVSS through ONVIF protocol.</p> <p> You are recommended to disable this function. Otherwise there might be security risks.</p>
Run Log	<p>After enabling it, you can view system running logs in <b>Intelligent Diagnosis &gt; Run Log</b>.</p>

System service	Description
Audio/Video Transmission Encryption	When this function is enabled, stream transmission will be encrypted.  You are recommended to enable this function. Otherwise you might risk data leakage.
RTSP over TLS	Enable this function to encrypt stream transmission. You are recommended to enable this function. Otherwise you might risk data leakage.
Private Protocol Authentication Mode	Select a private protocol authentication mode between security mode and compatible mode. Compatible mode is recommended.

**Step 3** Click **Save**.

## 6.6.5 Configuring Firewall

Enhance network and data security by prohibiting Ping and half-connection.

- **PING Prohibited:** When **PING Prohibited** is enabled, the device does not respond to Ping requests.
- **Anti Half Connection:** When **Anti Half Connection** is enabled, and the device can provide service normally under half-connection attack.



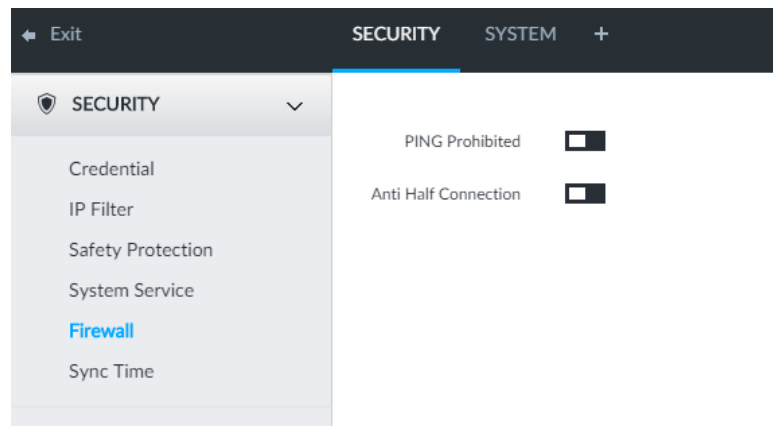
**Step 1** Click  or click  on the configuration page, and then select **SECURITY > Firewall**.

Figure 6-42 Firewall





**Step 2** Click  to enable PING Prohibited or Anti Hal Connection.

**Step 3** Click **Save**.

## 6.6.6 Configuring Time Synchronization Permission

Configure permissions of time synchronization actions from other devices or servers.

**Step 1** Click  or click  on the configuration page, and then select **SECURITY > Synch Time**.

**Step 2** Click  to enable time synchronization restriction.

**Step 3** Select **Allowlist** or **Blocklist**.

- Hosts in the allowlist have the permission to synchronize time of the Device.
- Hosts in the blocklist cannot synchronize time of the Device.

**Step 4** On the **Allowlist** page or the **Blocklist** page, add hosts.

1) Click **Add**. The following page is displayed.

Figure 6-43 Add a host





2) Select an IP version, and then enter an IP address.

3) Click **OK**.

**Step 5** Click **Save**.

You can also perform the following functions after configuring the allowlist or blocklist.

Table 6-14 Other functions

Function	Description
Edit IP address	Click  to edit IP address.
Delete IP address	Click  to delete a host from the list.
Configure IP address permission	Click the corresponding  of each host, so as to enable the allowlist or blocklist configuration for the host. Click  to disable the allowlist or blocklist configuration for the host.

## 6.7 Account Management

Device account adopts two-level management mode: user and user group. You can manage their basic information. To conveniently manage the user, we recommend the general user authorities shall be lower than high-level user authorities.



- To ensure device safety, enter correct login password to operate on the **Account** page (for example, add or delete user).
- After a correct login password is entered on the **Account** page, if you do not close the **Account** page, you can do other operations directly. If you close the page and enter it again, you shall enter the correct login password again.

### 6.7.1 User Group

Different users might have different authorities to access the device. You can divide the users to different groups. It is easy for you to maintain and manage the user information.

- System supports maximum 64 user groups. User group name supports maximum 64 characters.
- System has two default user groups (read-only): admin and ONVIF.
- Create new user group under the root.

## 6.7.1.1 Adding User Group




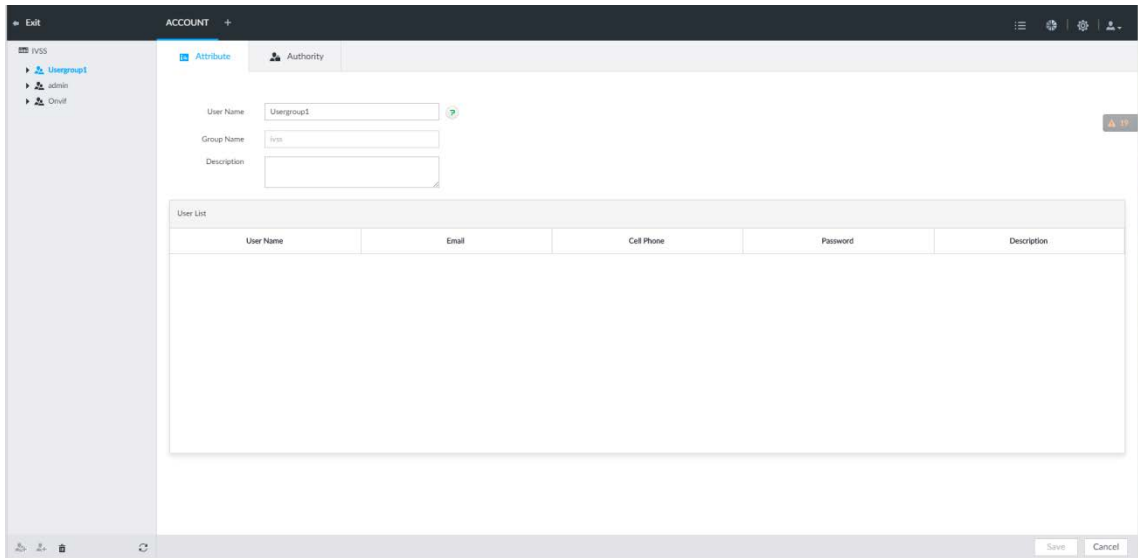
- Step 1** Click , or click  on the configuration page, and then select **ACCOUNT**.
- Step 2** Select the root node in the device tree on the left and then click  at the lower-left corner.
- Step 3** Enter current user's login password, and then click **OK**.  
System creates one user group and displays the **Property** page.

Figure 6-44 User group property



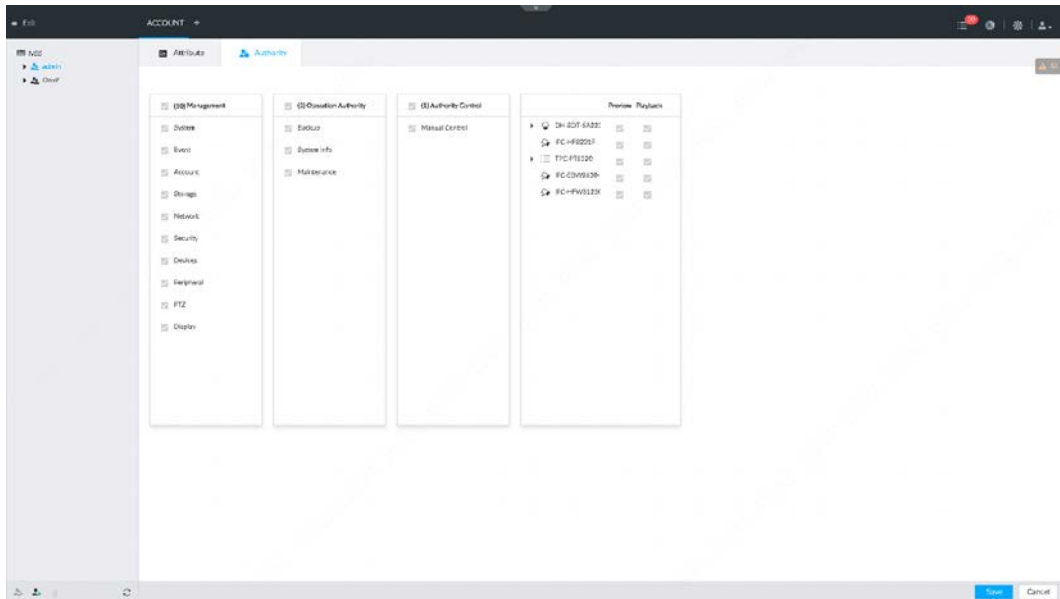
- Step 4** Set parameters.

Table 6-15 User group

Parameters	Description
Name	Set user group name. The name ranges from 1 to 64 characters. It can contain English letters, number and special character ("_", "@", ".").
Group name	Displays user group organization node. System automatically recognizes the group name.
Description	Enter user group description information.
User list	Displays user information of current group.

- Step 5** Select user authority.  
1) Click **Authority** tab.

Figure 6-45 Authority



2) Set user group authorities according to actual situation.

- : means it has the corresponding authority.
- Check the box at the top of the authority list (such as (0) Authority Control) to select all authorities of current category.

**Step 6** Click **Save**.

## 6.7.1.2 Deleting User Group



- Before you delete a user group, delete all users of current group first. User group cannot be restored after being deleted. Be cautious.
- Admin and ONVIF user cannot be deleted.

**Step 1** Click or click on the configuration page, and then select **ACCOUNT**.

**Step 2** Select user group and click .

**Step 3** Enter current user's login password, and then click **OK**.

**Step 4** Click **OK** on the prompt page.

## 6.7.2 Device User

The device user is to access and manage the device. System default administrator is admin. It is to add a user and then set corresponding authorities, so that the user can access the resources within its own rights range only.



User authorities adopt the user group authorities settings. It is read-only.

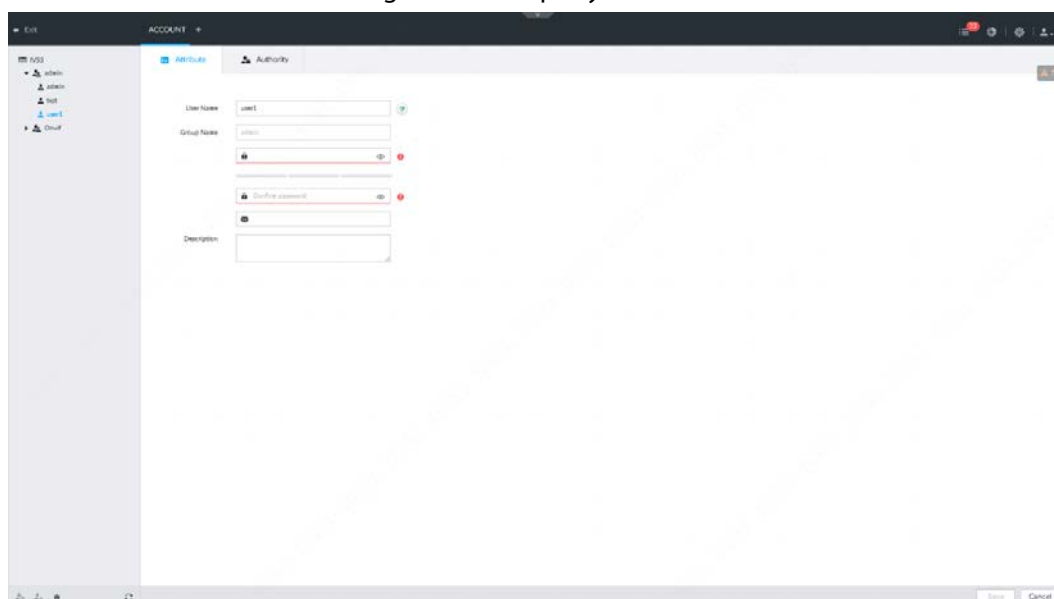
### 6.7.2.1 Adding a User

**Step 1** Click or click on the configuration page, and then select **ACCOUNT**.

**Step 2** Select admin user group or other newly added user group, and then click at the lower-left corner.

**Step 3** Enter current user's login password, and then click **OK**.

Figure 6-46 Property



**Step 4** Set parameters.

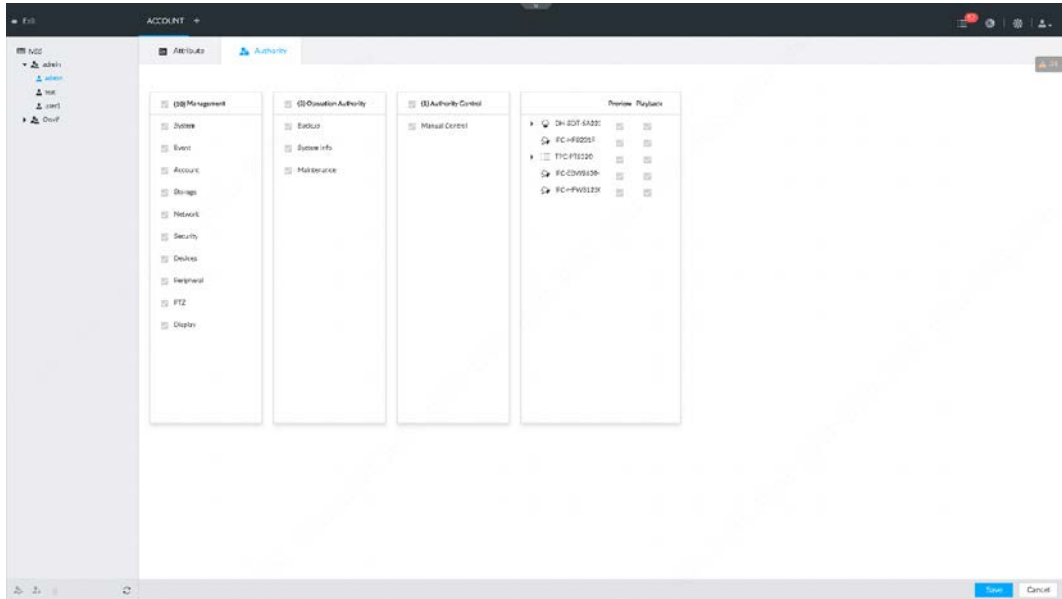
Table 6-16 User management

Parameters	Description
Name	Set user name. The name ranges from 1 to 31 characters. It can contain English letters, number and special character ("_", "@", ".").
Group name	Displays user organization node. System automatically identifies it.
Password	In the new password box, enter the new password and enter it again in the Confirm Password box.
Confirm Password	The password ranges from 8 to 32 non-empty characters. It can contain letters, numbers and special characters (excluding ";;& and space) .The password shall contain at least two categories. Usually we recommend the strong password.
Description	Enter user description information.

**Step 5** (Optional) Click **Authority** tab to view user authority.



Figure 6-47 Authority



**Step 6** Click **Save**.



### 6.7.2.2 Operation

After adding a user, you can modify user information or delete the user.



The user with account management authority can change its own and other users' information.

Table 6-17 User operation

Name	Operation
Edit user information	Select a user from user list. The <b>Property</b> page of the user is displayed, and the user's login password and description information can be modified.
Delete User	<p>Select a user from user list, and then click  to delete.</p> <p></p> <ul style="list-style-type: none"> <li>Before deleting an online user, block the user first. For details, see "7.6 Online User".</li> <li>User information cannot be restored after being deleted. Be cautious.</li> </ul>


### 6.7.3 Password Maintenance

Maintain and manage user's login password.

#### 6.7.3.1 Modifying Password

Modify user's login password.

##### 6.7.3.1.1 Modifying Password of the Current User

**Step 1** Click  at the top right corner, and then select **Modify Password**.

Step 2 Enter the old password, the new password and then confirm.

Step 3 Click OK.

### 6.7.3.1.2 Modifying Password of Other User

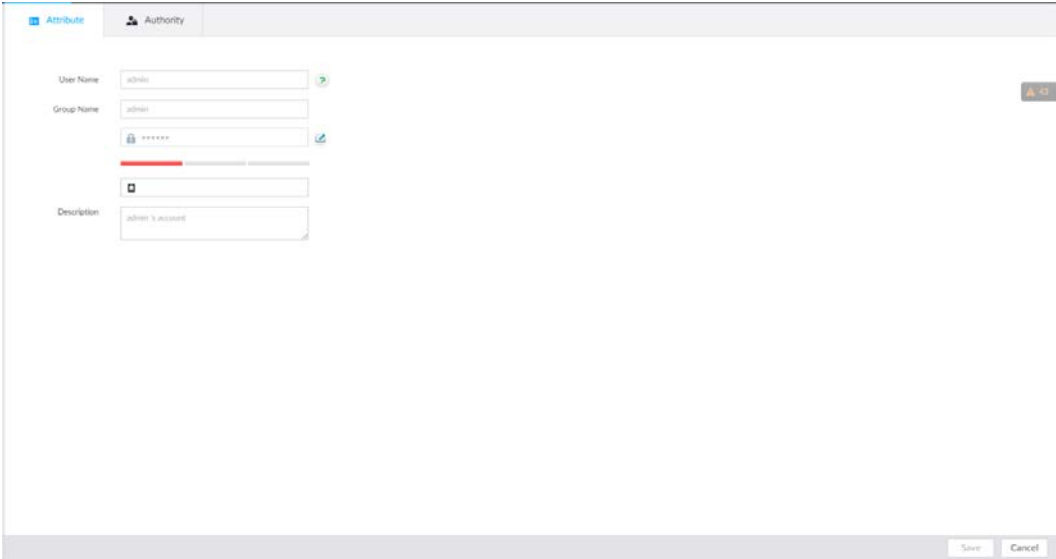


Only **Admin** account supports this function.


Step 1 Click  or click  on the configuration page, and then select **ACCOUNT**.

Step 2 Select a user.

Figure 6-48 Property

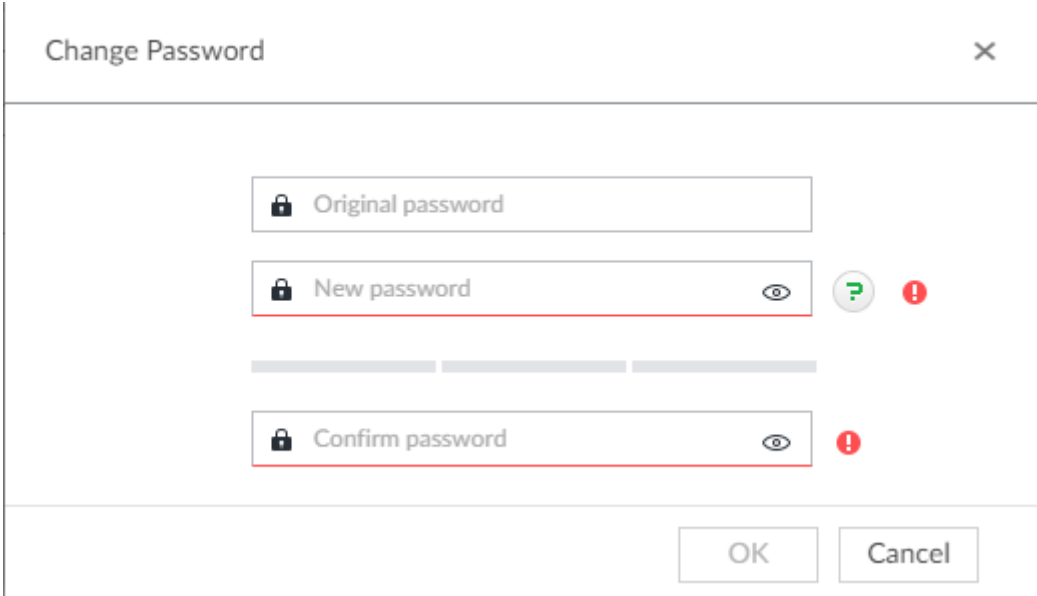


The screenshot shows a web interface with a tab labeled 'Authority'. It contains several input fields: 'User Name' with the value 'admin', 'Group Name' with the value 'admin', a password field with masked characters '\*\*\*\*\*', a field with a lock icon, and a 'Description' field with the value 'admin's account'. There are 'Save' and 'Cancel' buttons at the bottom right.

Step 3 Click .

Step 4 Enter current user's login password, and then click **OK**.  
The **Change Password** page is displayed.

Figure 6-49 Modify password



The screenshot shows a 'Change Password' dialog box with three password input fields: 'Original password', 'New password', and 'Confirm password'. Each field has a lock icon and a visibility icon. The 'New password' and 'Confirm password' fields have a red border and a red exclamation mark icon, indicating a warning. There are 'OK' and 'Cancel' buttons at the bottom.

Step 5 In the **New Password** box, enter the new password and enter it again in the **Confirm Password** box.

Step 6 Click OK.

## 6.7.3.2 Resetting Password



You can use email address or answer the security questions to reset password once you forgot it. You can only reset password on the local interface of the Device.



When password resetting function is not enabled, the password cannot be reset if the security questions are not set.

### 6.7.3.2.1 Leaving Email Address and Security Questions

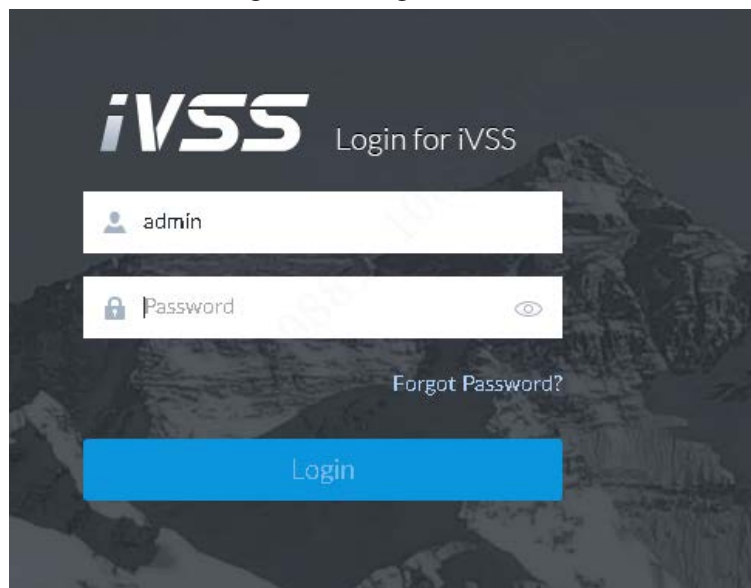
Enable the password reset function, leave an email address and set security questions. You can only use the local interface to set security questions.

- Step 1** Click  or click  on the configuration page, and then select **ACCOUNT**.
- Step 2** Select the root node in the device tree on the left.
- Step 3** Click  to enable the password reset function.
- Step 4** Enter an email address for resetting password.
- Step 5** Set security questions. Only available on the local interface of the Device.
- Step 6** Click **Save**.

### 6.7.3.2.2 Resetting Password on Local Interface

- Step 1** Connect a display to the Device, and then go to the **Login** page of device.

Figure 6-50 Login



- Step 2** Click **Forgot Password**.

- Step 3** Click **OK**.

- If you have set the email address information, the QR code page is displayed.
- If you have not set the email address information, the email address page is displayed. After you set the email address information and click **Next**, the QR code page is displayed.

Figure 6-51 Enter email address

Reset Password

1 Password Protection 2 Retrieve Password 3 Set New Password

Email (To reset password)

Email

Next Cancel

Figure 6-52 Scan QR code

Reset Password

1 Retrieve Password 2 Set New Password

Retrieve Password By Email

SN \*\*\*\*\*Q00019

Scan QR Code

Scan the code on your current interface

1. Use specified APP (DMSS) to scan, APP can automatically send out the data to the server  
2. Use non-specified APP to scan, please send QR Code to support\_rpwd@global.dahuatech.com

Use specified APP to scan, security code will send to 1\*\*\*@qq.com Email

Input Security Code ?

Next Cancel

Step 4 Reset the password.

Figure 6-53 Security questions

Reset Password

1 Retrieve Password 2 Set New Password

Retrieve Password

---

Question 1

\* Answer

Question 2

\* Answer

Question 3

\* Answer

Next Cancel

**Step 5** Click **Next**.

Figure 6-54 New password setting

Reset Password

1 Retrieve Password 2 Set New Password

---

Confirm Modify Cancel

**Step 6** Set parameters.

Table 6-18 Description of password parameters

Parameters	Description
User	The default user name is admin.
Password	In the <b>New Password</b> box, enter the new password and enter it again in the <b>Confirm Password</b> box.
Confirm Password	The new password can be set from 8 through 32 non-empty characters and contains at least two types from number, letter and special characters (excluding "';:& and space). Enter a strong password according to the password strength indication.

Parameters	Description
Prompt question	<p>After setting the prompt, when you move the mouse to on the login page, the system pops up a prompt to help you remember the password.</p> <p>The prompt question function is for local login page only. See the actual page for detailed information.</p>

**Step 7** Click **Confirm Modify**.

You can log in with the new password.

## 6.7.4 ONVIF

When the remote device is connecting with the device through ONVIF protocol, use the verified ONVIF account.



- System adopts three ONVIF user groups (admin, user and operator). You cannot add ONVIF user group manually.
- You cannot add user under ONVIF group directly.


### 6.7.4.1 Adding ONVIF User

**Step 1** Click  or click  on the configuration page, and then select **ACCOUNT**.

**Step 2** Select user group under ONVIF.

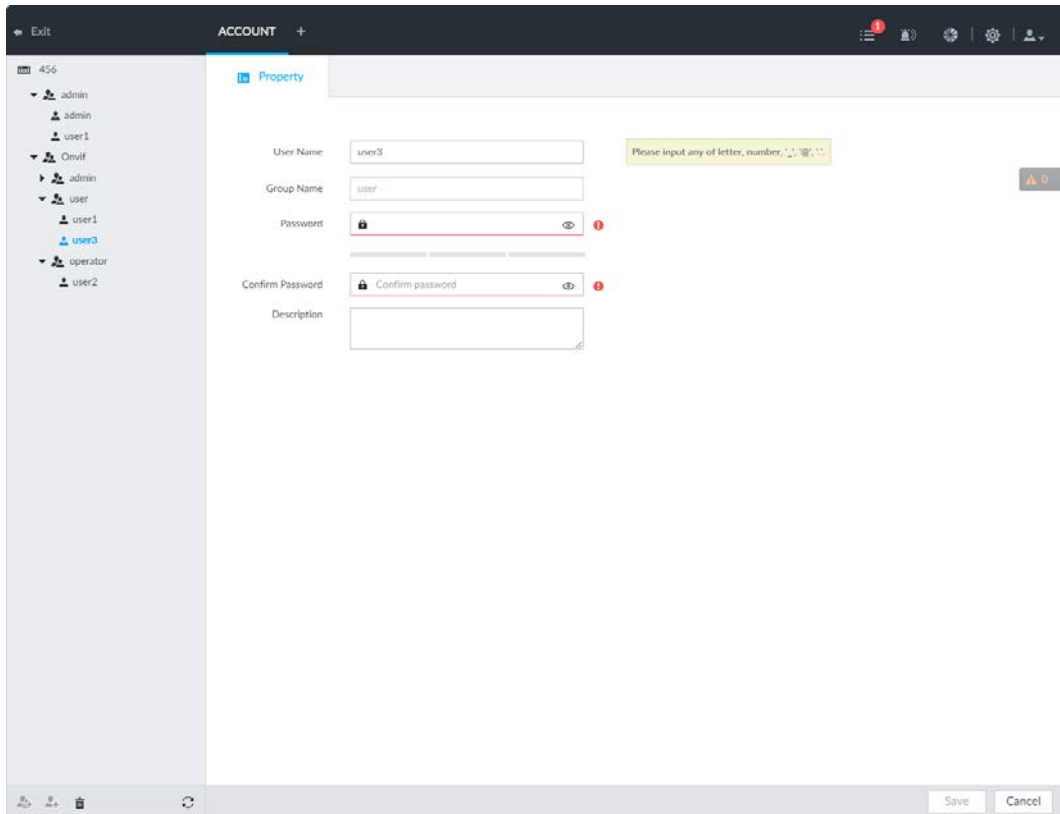
Figure 6-55 ONVIF

User Name	Password	Description
admin	→	→
user	→	→
operator	→	→

**Step 3** Click  at the lower-left corner of the **Property** page.

**Step 4** Enter the login password of current user, and then click **OK**.

Figure 6-56 ONVIF property



**Step 5** Set parameters.

Table 6-19 ONVIF parameters description

Parameters	Description
User Name	Set ONVIF user name. The name ranges from 1 to 31 characters. It can contain English letters, number and special character ( _ @ .).
Group name	Displays user organization node. System automatically identifies it.
Password	Set ONVIF user password.
Confirm Password	The password ranges from 8 to 32 non-empty characters. It can contain letters, numbers and special characters (excluding " " ; & and space) .The password shall contain at least two categories. Usually we recommend the strong password.
Description	Enter ONVIF user description information.

**Step 6** Click **Save**.

### 6.7.4.2 Deleting ONVIF User



Deleting the admin account is not supported.

**Step 1** Click , or click  on the configuration page, and then select **ACCOUNT**.

**Step 2** Select ONVIF and click .

**Step 3** Enter current user's login password, and then click **OK**.  
The following prompt page is displayed.

**Step 4** Click **OK**.

## 6.8 System Configuration



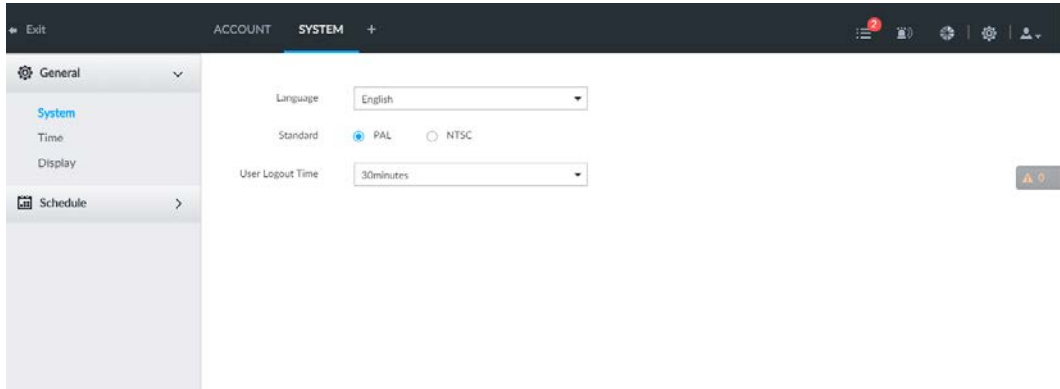
Click  or click  on the configuration page, select **SYSTEM**. The **SYSTEM** page is displayed. Set system basic settings, such as general parameters, time, display parameter, schedule, and voice.

Figure 6-57 System management



### 6.8.1 Setting System Parameters

Set system language, standard, user logout time, virtual keyboard, and mouse moving speed.



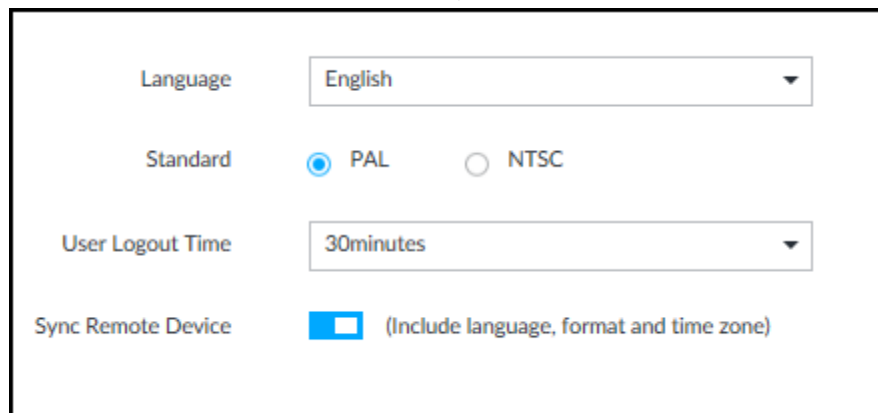

**Step 1** Click  or click  on the configuration page, and then select **SYSTEM > General > System**.

Figure 6-58 Configuring system settings





**Step 2** Set parameters.

Table 6-20 System parameters description

Parameters	Description
Language	Set system language.
Standard	<p>Select video standard.</p> <ul style="list-style-type: none"> <li>• PAL is mainly used in China, Middle East and Europe.</li> <li>• NTSC is mainly used in Japan, United States of America, Canada and Mexico.</li> </ul> <p> As a technical standard of processing video and audio signals, PAL and NTSC mainly differ in encoding, decoding mode and field scanning frequency.</p>



Parameters	Description
User Logout Time	Set auto logout interval once you remain inactive for a specified period or the device exceeds the set value. After auto logout, the user needs to login again to operate. If you select No Logout, system does not automatically log out.
Sync Remote Device	Click <input type="checkbox"/> to enable the function. If enabled, the language, standard and time settings configured here will be synchronized to all the connected remote devices.
Virtual Keyboard	Enable virtual keyboard function on the local menu. See "Appendix 1.2 Virtual Keyboard" for detailed information.  This function is for local menu only.
Mouse Moving Speed	Set mouse moving speed on the local interface.  This function is for local menu only.

**Step 3** Click **Save**.

## 6.8.2 System Time

Set system time, and enable NTP function according to your need. After enabling NTP function, device can automatically synchronize time with the NTP server.




**Step 1** Click  or click  on the configuration page, and then select **SYSTEM > General > Time**.

Figure 6-59 Time



Date  
2019.12.30

Time  
16:04:57

Time  Manual Setting

Date/Time

Sync with Internet Time Server

Server

Auto Sync Time Interval

Time and Date Format

Time Zone

AutoTimeSynchronization

DST

Enable


Type  Date  Week

Start

End

**Step 2** Set parameters.

Table 6-21 System parameters description

Parameters	Description
Time	Set system date and time. You can set manually or set device to synchronize time with the NTP server. <ul style="list-style-type: none"><li>• <b>Manual Setting:</b> Select <b>Manual Setting</b> and then set the actual date and time in the following two ways.<ul style="list-style-type: none"><li>◇ Click , and then set the time and date in the calendar.</li><li>◇ Click <b>Sync</b> to synchronize device time with your PC.</li></ul></li><li>• <b>Sync with the Internet Time Server:</b> Select the check box, enter NTP server IP address or domain, and then set <b>Auto Sync Time Interval</b>.</li></ul>
Time and Date Format	Set time and date display format.
Time Zone	Set device time zone.
Auto Time Synchronization	After enabling this function, IVSS detects system time of remote device once in every interval. When time of remote device is inconsistent with IVSS time, IVSS will calibrate the time of remote device automatically.

**Step 3** (Optional) Set DST.



DST is a system to stipulate local time, in order to save energy. If the country or region where the device is located follows DST, you can enable DST to ensure that system time is correct.

- 1) Click  to enable DST.
- 2) Select DST mode. It includes **Date** and **Week**.
- 3) Set DST start time and end time.

**Step 4** Click **Save**.

## 6.8.3 Display

Set connected display resolution and refresh rate.



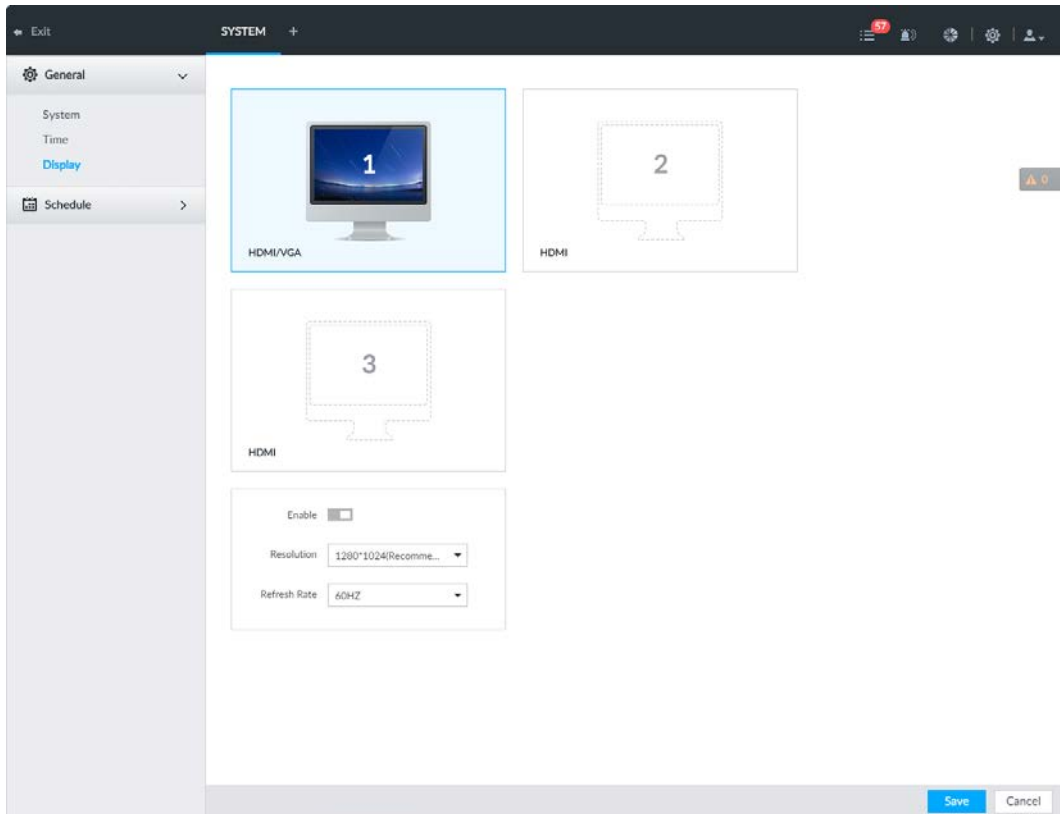




- Step 1** Click , or click  on the configuration page, and then select **SYSTEM > General > Display**.

Figure 6-60 Display



- SN 1–3 refers HDMI 1–HDMI 3. Among which, HDMI/VGA is the main display, while the VGA and HDMI 1 outputs the same video.
- VGA and HDMI 1 are outputting the same video source. Three HDMI ports can output different video sources.
-  means display is connected and enabled.  means display is connected but has not enabled.  means display is disconnected.

**Step 2** Select a display.

**Step 3** Click  to enable the selected display.

**Step 4** Set parameters.

Table 6-22 Display parameters description

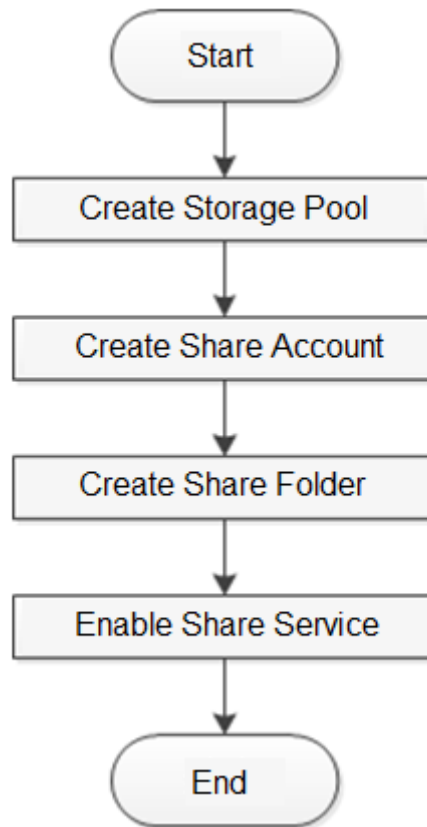
Parameters	Description
Resolution	Set display resolution. Different displays support different resolutions. See your actual page for detailed information.
Refresh rate	Set refresh rate of the display.

**Step 5** Click **Save**.

## 6.9 IPSAN

IPSAN is a storage technology based on IP network. After you create a storage pool, you can share your storage directory with other devices through iSCSI.

Figure 6-61 Configuring IPSAN



## 6.9.1 Creating Storage Pool



Storage pool is a logical storage space after the storage device is virtualized. It is managed by the system, and can be composed of multiple actual disks or RAID. IPSAN is one of the major means to realize storage virtualization.



Be careful that creating storage pool will format the disk.

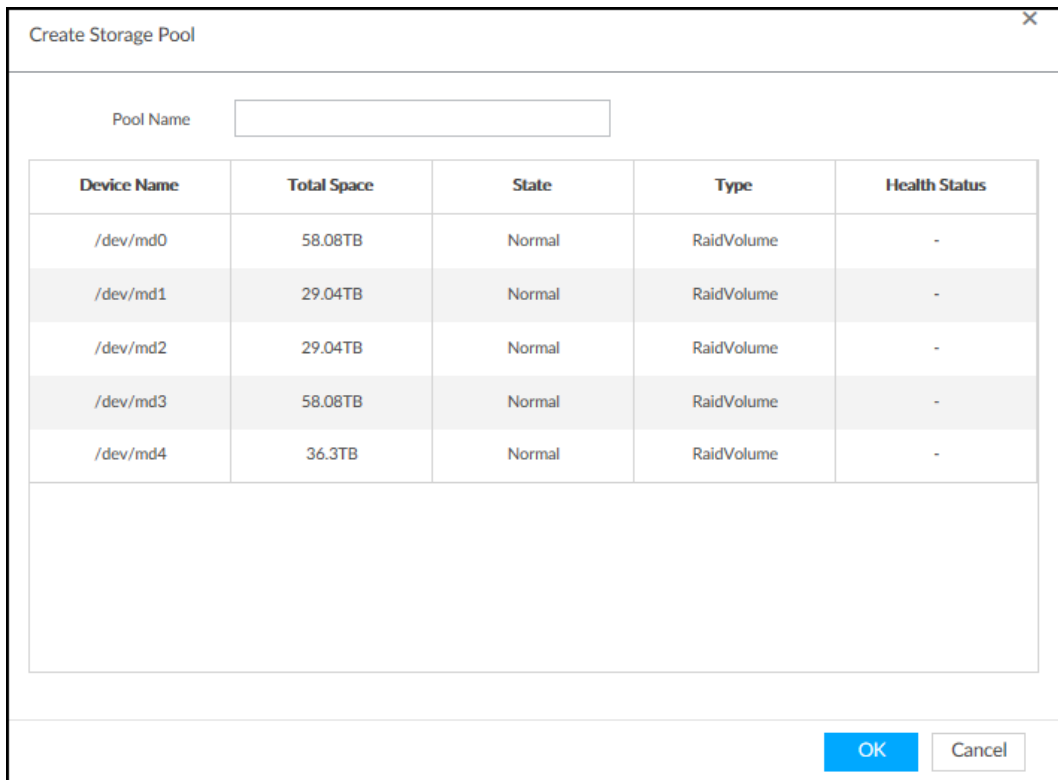
**Step 1** Click  or click  on the configuration page, and then select **IPSAN > Storage Pool**.

Figure 6-62 Storage pool

Storage Pool	Members	Total Space	Used Space	State	Edit
storage1	/dev/sd*	5586.02GB	5.00GB	Normal	
all	/dev/sd*	5586.04GB	432GB	Normal	

**Step 2** Click **Add**.

Figure 6-63 Create storage pool



**Step 3** Name the pool, and then select a disk or RAID group.



By default, in the **Device Name** column, "sdx" (x ranges from a to z) is a disk, such as /dev/sda, and "mdx" (x is number) is a RAID group, such as /dev/md0.

**Step 4** Click **OK**.

The confirmation dialogue box is displayed.

**Step 5** Click **OK**.

The system starts to create storage pool.



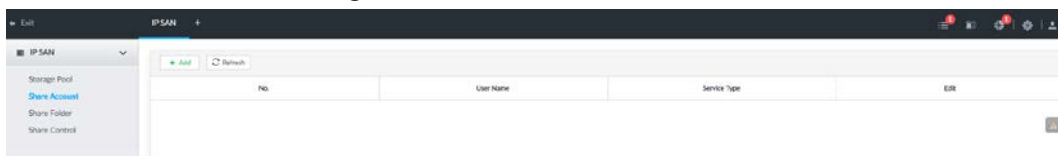
To delete a pool, click . To refresh the storage pool list, click **Refresh**.

## 6.9.2 Managing Share Account

Use share account to access the shared folder.

**Step 1** Click or click on the configuration page, and then select **IPSAN > Share Account**.

Figure 6-64 Share account




**Step 2** Click **Add**.

Figure 6-65 Add user

**Step 3** Set parameters.

Table 6-23 Parameters description

Parameters	Description
User Name	Name the user.
Service Type	You can add an iSCSI share user.
Password	Set a password for the user
Confirm password	 The password shall be 12-digit if the service type is iSCSI.
Remark	Set the remark information for identifying the user.

**Step 4** Click OK.

## 6.9.3 Configuring Share Folder

Configure the share folders that other users can access remotely.



















**Step 1** Click  or click  on the configuration page, and then select **IPSAN > Share Folder**.

Figure 6-66 Share folder



Director Name	Free Space/Total	Pool Name	Share Type	Share User	State	Description	Edit
33333	100GB/100GB	aaa	NONE		Active		 
44444	100GB/100GB	aaa	NONE		Active		 
55555	100GB/100GB	aaa	NONE		Active		 
66666	100GB/100GB	aaa	NONE		Active		 
77777	100GB/100GB	aaa	NONE		Active		 
www@q13	300GB/200GB	cn@ch@1	NONE		Active		 
www@q132	300GB/200GB	cn@ch@1	NONE		Active		 
www@q133	200GB/200GB	cn@ch@1	NONE		Active		 


**Step 2** Click Add.

Figure 6-67 Add (iSCSI)

**Step 3** Set parameters.



Table 6-24 Parameters description

Parameters	Description
Directory Name	Name the folder.
Port Name	Select a pool.  The available free space of the selected pool is displayed beside the pool name.
Share Capacity	Set the space of the folder.
Block Size	Set the block size of the folder, such as 512 Byte, 1024 Byte, 2048 Byte and 4096 Byte.  You need to set block size when the service type is iSCSI.
Description	(Optional) Describe the folder for the ease of identifying it.
Share Type	You can only select iSCSI.

Parameters	Description
Cache Type	<p>Set the cache strategy of the share folder, including <b>Write-back</b> and <b>Direct-write</b>.</p> <ul style="list-style-type: none"> <li>• <b>Direct-write:</b> Write data directly into the disk and refresh the cache data. You are recommended to select direct-write when you have less data to store and have a high requirement for data integrity.</li> <li>• <b>Write-back:</b> Write data into the cache, and then store it into the disk when the cache is full or system is available. You are recommended to select write-back when you have much more data to store and have a low requirement for data integrity.</li> </ul> <p> You need to select the cache type when the service type is iSCSI.</p>

**Step 4** Click **OK**.



- The system forces to disable automatic maintenance the first time you create a share folder, or when you create a folder when automatic maintenance is enabled automatically. Once you have configured IPSAN, you can manually enable automatic maintenance.
- Click  to delete a share folder; click  to edit a share folder; click **Refresh** to refresh the current configuration.
- Modifying cache type takes effect after the Device restarts.

## 6.9.4 Share Control

Users can access the share folders only when the share service is enabled.

**Step 1** Click , or click  on the configuration page, and then select **IPSAN > Share Control**.

Figure 6-68 Share control



**Step 2** Click  to enable share service; click  to enable share service.

**Step 3** Click **OK**.

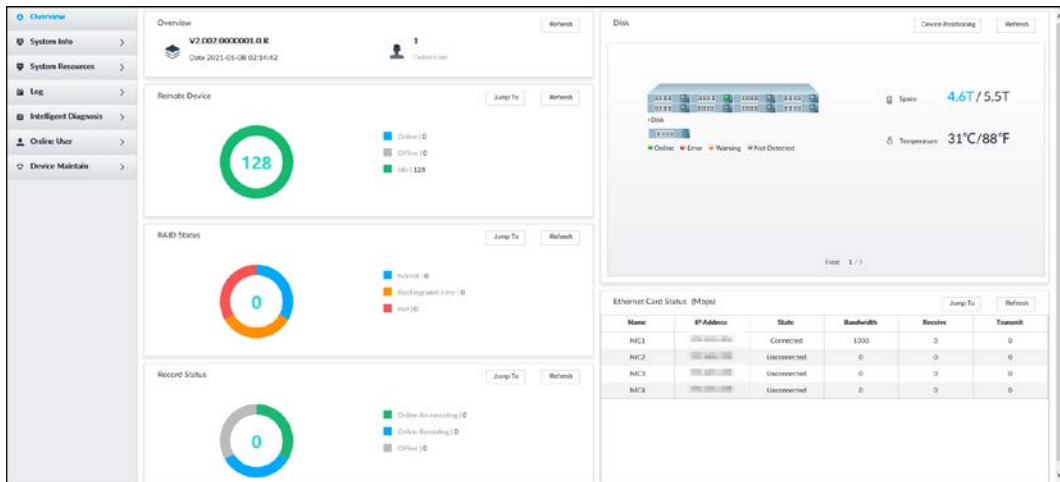


# 7 System Maintenance

Click **+** on the **LIVE** page, and select **MAINTAIN**.

You can operate and maintain the device working environment to guarantee proper operation.

Figure 7-1 Maintain



## 7.1 Overview

Click **+** on the **LIVE** page, and select **MAINTAIN > Overview**.

Figure 7-2 Overview

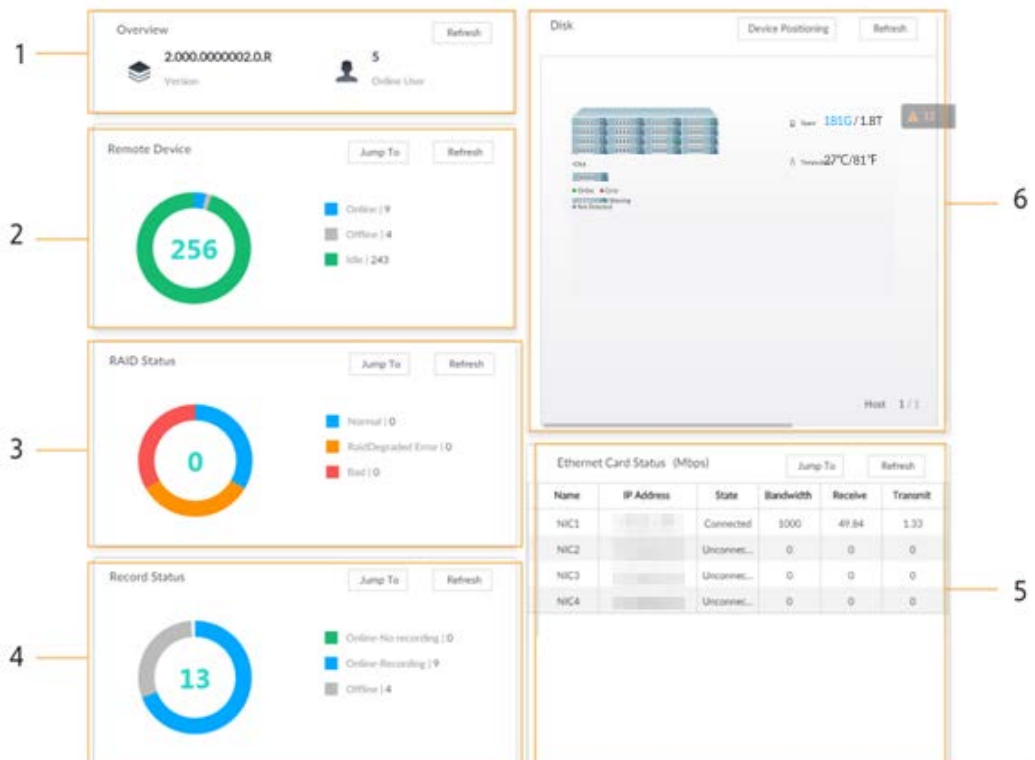





Table 7-1 Overview

No.	Function	Description
1	Overview	View device version details and online users. Click <b>Refresh</b> to refresh the data.
2	Remote Device	View the connection and idle status of remote devices <ul style="list-style-type: none"> <li>Click <b>Jump To</b> to go to the <b>DEVICE</b> page for detailed information.</li> <li>Click <b>Refresh</b> to refresh the data.</li> </ul>
3	RAID Status	View RAID status. <ul style="list-style-type: none"> <li>Click <b>Jump To</b> to go to the <b>STORAGE</b> page for detailed information.</li> <li>Click <b>Refresh</b> to refresh the data.</li> </ul>
4	Record Status	View recording status of remote devices. <ul style="list-style-type: none"> <li>Click <b>Jump To</b> to go to the <b>VIDEO RECORDING</b> page for detailed information.</li> <li>Click <b>Refresh</b> to refresh the data.</li> </ul>
5	Ethernet Card Status (Mbps)	View NIC status. <ul style="list-style-type: none"> <li>Click <b>Jump To</b> to go to the <b>TCP/IP</b> page for detailed information.</li> <li>Click <b>Refresh</b> to refresh the data. <ul style="list-style-type: none"> <li>◇  indicates that the disk is online.</li> <li>◇  indicates that the disk is exception.</li> <li>◇  indicates that the slot has no disk.</li> </ul> </li> </ul>
6	Disk	View disk status, device temperature and storage usage. <ul style="list-style-type: none"> <li>Click <b>Device Positioning</b>, and then the device positioning indicator flashes. In this way, you can quickly find the device.</li> <li>Click <b>Refresh</b> to refresh the data.</li> </ul>

## 7.2 System Resources

View device and AI module information.


### 7.2.1 Viewing Device Information

Click  on the **LIVE** page, and select **MAINTAIN > System Resources > DEVICE INFO**.

The **System Resources** page is displayed. You can view resource status including CPU and memory usage, panel temperature and fan speed.

Figure 7-3 System resources

Detection Item	Type	Value
Memory	Used Space/Total Space	2.35GB/7.67GB
CPU	CPU Usage	7%
MainboardFan1	Fan Speed	1890r/min
MainboardFan2	Fan Speed	1829r/min
Mainboard1	Temperature	42°C
Mainboard2	Temperature	33.5°C
Mainboard3	Temperature	33.75°C
Mainboard4	Temperature	34.75°C
CPU	Temperature	38°C

- Click  to filter the search conditions.
- Click **Refresh** to refresh the data.

## 7.2.2 Viewing AI Module Information


Click  on the **LIVE** page, and select **MAINTAIN > System Resources > AI Module Info**. You can view status of the AI modules.

Figure 7-4 AI module information

Name	State
IntelModule_1	

Total 1 item(s) Show up to 10

1/1 1/1 GO

## 7.3 System Information

### 7.3.1 Viewing Legal Information

View device software license, privacy policy, and open-source software note.

Click  on the **LIVE** page, and select **MAINTAIN > System Info > Legal Info**.

### 7.3.2 Viewing Algorithm Version

View device algorithm license status and AI version information.

Click  on the **LIVE** page, and select **MAINTAIN > System Info > Algorithm Version**.



Figure 7-6 System log

Type	Level	Time	Description
SyncSystemTime	Notice	2019-12-30 15:00:00	OffTime:2019-12-30 15:00:00; NewTime:2019-12-30 16:00:00; IP Address:171.35.0.46
SyncSystemTime	Notice	2019-12-30 15:41:46	OffTime:2019-12-30 15:41:46; NewTime:2019-12-30 15:41:46; IP Address:171.35.0.46
SyncSystemTime	Notice	2019-12-30 15:40:43	OffTime:2019-12-30 15:36:00; NewTime:2019-12-30 15:40:43; Record Type:WebSD; IP Address:30.172.33.11
Task is paused.	Notice	2019-12-30 13:48:42	Task Name:ynrno, 11.
Task is started.	Notice	2019-12-30 13:56:45	Task Name:ynrno, 11.
Task is paused.	Notice	2019-12-30 13:36:17	Task Name:ynrno, 11.
Task is started.	Notice	2019-12-30 13:35:55	Task Name:ynrno, 11.
Task is paused.	Notice	2019-12-30 13:33:48	Task Name:ynrno, 11.
Task is started.	Notice	2019-12-30 13:33:22	Task Name:ynrno, 11.
SyncSystemTime	Notice	2019-12-30 12:52:02	OffTime:2019-12-30 12:52:02; NewTime:2019-12-30 12:52:02; IP Address:171.35.0.46
StartUp	Error	2019-12-30 12:53:22	Flag ExitPowerFull.
Abort	Error	2019-12-30 12:53:22	Time:2019-12-30 12:50:55.
SyncSystemTime	Notice	2019-12-30 12:47:48	OffTime:2019-12-30 12:47:48; NewTime:2019-12-30 12:47:48; IP Address:171.35.0.46
StartUp	Error	2019-12-30 12:46:58	Flag ExitPowerFull.
Abort	Error	2019-12-30 12:46:58	Time:2019-12-30 12:45:52.
SyncSystemTime	Notice	2019-12-30 09:53:19	OffTime:2019-12-30 09:53:19; NewTime:2019-12-30 09:53:19; IP Address:171.35.0.46
SyncSystemTime	Notice	2019-12-29 16:00:00	OffTime:2019-12-29 15:59:57; NewTime:2019-12-29 16:00:00.

### 7.4.3 Operation

Search, export and clear log.

Table 7-3 Log operation

Name	Operation
Export log	Click  to export log information to local PC or USB storage device.
Clear log	Click <b>Clear all</b> to clear all system logs.  You will be unable to track the system error reason if you clear log.

## 7.5 Intelligent Diagnosis

### 7.5.1 Run Log

View system running logs for troubleshooting.



Make sure that you have enabled **Run Log** in **SECURITY > System Service**. Otherwise there is no log data.

On the **LIVE** page, click , and select **MAINTAIN > Intelligent Diagnosis > Run Log**.

Figure 7-7 Logs

<input type="checkbox"/>	No.	Type	File Name	Operate
<input type="checkbox"/>	1	core	coredump/core-20191021142751@_JVSS2.000.0000002.0.R_172.12.1.101_123456789012345.gz	
<input type="checkbox"/>	2	core	coredump/core-20191021001805@_JVSS2.000.0000002.0.R_172.12.1.101_123456789012345.gz	
<input type="checkbox"/>	3	core	coredump/core-20191019220041@_JVSS2.000.0000002.0.R_172.12.1.101_123456789012345.gz	

- Click to export a log.
- After selecting multiple logs, click **Export** to export them in batches.

## 7.5.2 One-click Export

Export the diagnosis data for troubleshooting when the device is exception.

**Step 1** On the **LIVE** page, click **+**, and select **MAINTAIN > Intelligent Diagnosis > One-click Export**.

**Step 2** Click **Generate Diagnosis Data** to generate diagnosis data.

**Step 3** Click **Export** to export the diagnosis result.

## 7.6 Online User

Search remote access network user information or you can block a user from access for a period of time. During the block period, the selected user cannot access the Device.



Cannot block yourself or block admin.

**Step 1** On the **LIVE** page, click **+**, and select **MAINTAIN > Online User > Online User**. The **Online User** page is displayed.



The list displays the connected user information.

**Step 2** Block user.

- Block: Click **⊖** corresponding to the user.
- Batch block: Select multiple users you want to block and then click **Block**.

The **Block** page is displayed.

Figure 7-8 Block

Block

Block Time 30 Min

OK Cancel

**Step 3** Set block period. The default period is 30 minutes.

**Step 4** Click **OK** to save the configuration.

## 7.7 Device Maintenance

Device maintenance is to reboot device, restore factory default setup, or upgrade system and so on. It is to clear the malfunction or error during the system operation and enhance device running performance.

## 7.7.1 Upgrading Device

Upgrade device or the AI module version.

### 7.7.1.1 Upgrading the Device

You can import the upgrade file to upgrade device version. The upgrade file extension name shall be .bin.



- During upgrading, do not disconnect from power and network, and reboot or shut down the Device.

• Make sure that the upgrade file is correct. Improper upgrade file might result in device error! You need to obtain the correct upgrade file and save it in the corresponding path.

- When operating on the local interface, save the upgrade file in the USB storage device and then connect the USB storage device to the IVSS.
- When operating on the web or IVSS interface, save the upgrade file on the PC in which the Web or PCAPP is located.

**Step 1** On the **LIVE** page, click **+**, and select **MAINTAIN > Device Maintain > Upgrade > Host**.

**Step 2** Click **Browse** to select an upgrade file.

**Step 3** Click **Upgrade Now**.

**Step 4** Click **OK**.

The system starts upgrading. Device automatically reboots after successfully upgraded.

### 7.7.1.2 Viewing AI module

View the system version of the AI module installed on the device.

**Step 1** On the **LIVE** page, click **+**, and then select **MAINTAIN > Device Maintain > Upgrade > AI Module**.

Figure 7-9 Upgrade AI module

	Name	Upgrade State
<input checked="" type="checkbox"/> (1)	IntelliModule_7	--

**Step 2** View AI module status.

- indicates that the AI module is online.
- indicates that the AI module is not started.
- Blank row indicates that the AI module is disconnected.

## 7.7.2 Default

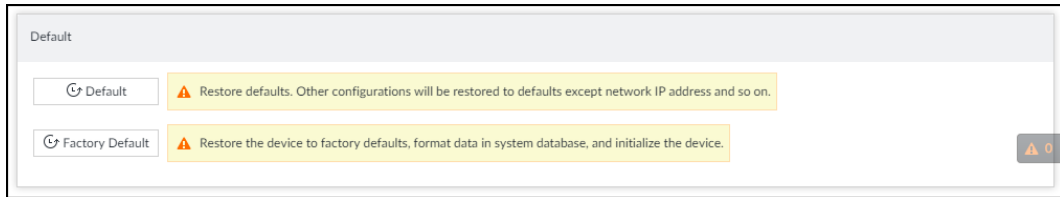
When the system runs slowly and has configuration errors, try to solve the problems by restoring the default settings.



All configurations are lost after factory default operation.

**Step 1** On the **LIVE** page, click **+**, and then select **MAINTAIN > Device Maintain > Default**.

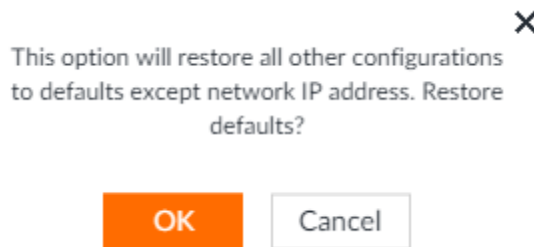
Figure 7-10 Default



**Step 2** Select a method.

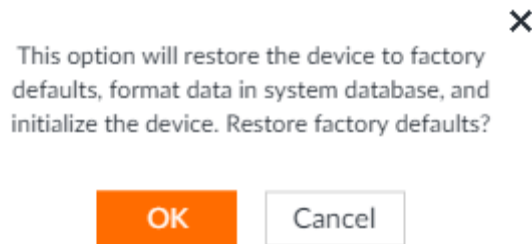
- Click **Default**.

Figure 7-11 Prompt (1)



- Click **Factory Default**.

Figure 7-12 Prompt (2)



**Step 3** Click **OK**.

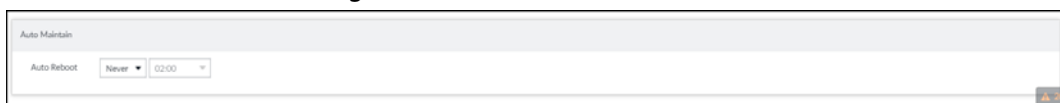
System begins to restore default settings. After successfully restored default settings, system prompts to restart the device.

## 7.7.3 Automatic Maintenance

If the device has run for a long time, you can set to automatically reboot the device at idle time.

**Step 1** On the **LIVE** page, click **+**, and then select **MAINTAIN > Device Maintain > Auto Maintain**.

Figure 7-13 Auto Maintain



**Step 2** Set auto reboot time.

**Step 3** Click **Save**.

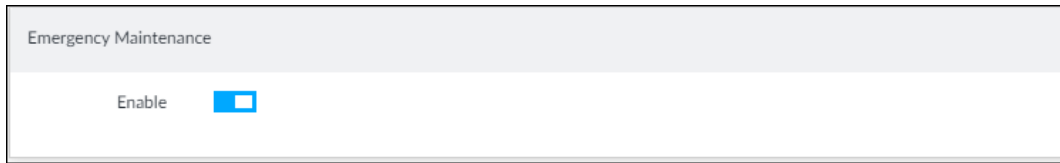
**Step 4** Enable **Emergency Maintenance**.

When the Device has an upgrade power outage, running error and other problems, and you cannot log in, you can enable **Emergency Maintenance** to restart, clear configuration,



and upgrade.

Figure 7-14 Emergency Maintenance



## 7.7.4 IMP/EXP

Export device configuration file to local PC or USB storage device, to backup it. When the configuration is lost due to abnormal operation, import the backup configuration file to restore system configurations quickly.

On the **LIVE** page, click **+**, and then select **MAINTAIN > Device Maintain > IMP/EXP**. The **IMP/EXP** page is displayed.

Figure 7-15 IMP/EXP



### Exporting Configuration File

Click **Export** to export configuration file to local PC or USB storage device. File path might vary depending on your operations.

- On PCAPP, click **☰**, and then select **Download** to view file saving path.
- Select file saving path during local operation.



Connect USB device to the system if you are on the local menu to operate.

- During web operations, files are saved under default downloading path of the browser.

### Importing Configuration File

Click **Browse** to select the configuration file, and then click **Import**. After the configuration file is imported successfully, the device will reboot automatically.

# 8 PCAPP Introduction

After installing PCAPP, system supports to access the Device remotely to carry out system configuration, function operations and system maintenance.



For details about installing PCAPP, see "5.3.1 Logging in to PCAPP Client".

## 8.1 Interface Description











Double-click  on the PC desktop. System displays PCAPP at full screen by default. Click  to display the task column.

Figure 8-1 IVSS task column



Table 8-1 Icons

Icons	Description
	Address bar: Enter the IP address of remote device.
	Enter device IP address and then click the button to go to the login page. Now the icon turns into  . Click to refresh the page.
	Click to view history login record, view downloads, set compatibility mode and view IVSS version information.
	Click to minimize PCAPP.
	Click to maximize PCAPP.
	Click to display PCAPP at full screen.
	Click to close PCAPP.


## 8.2 History Record

Click , and then select **History**.

You can view history access record and clear buffer.

- Click **Clear History** to clear all history records.
- Click **Clear Buffer** to clear buffer data, and reboot PCAPP.

## 8.3 Viewing Downloads

To view and clear history downloads, click , and then select **Downloads**. The **Downloads** page is displayed.

- Double-click file name to open it.
- Click **Displayed in Folder** to open the folder where the file is located.

- Click **Clear Downloads** to clear history download records.

## 8.4 Configuring PCAPP

When PC theme is not Aero, video of PCAPP might not be displayed normally. It is suggested that PC theme should be switched to Aero, or compatibility mode of PCAPP should be enabled.

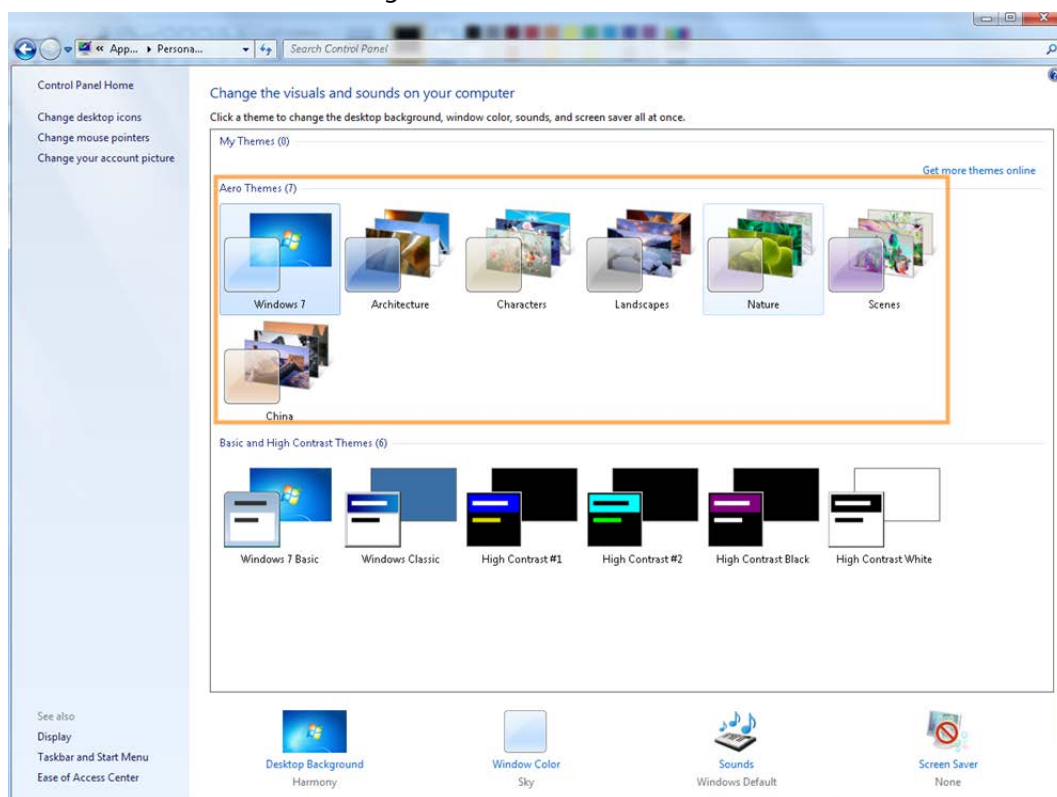
### Switching PC Theme



This section takes Windows 7 as an example.

Right-click any blank position on PC desktop, select **Personalize**, and then switch to Aero theme. Restart the PCAPP before the Aero theme takes effect.

Figure 8-2 PC theme



### Setting Video and Picture Storage Path

Click **Browse** to specify the paths for saving videos and pictures. Only PCAPP supports this function.

### Enabling Compatibility Mode


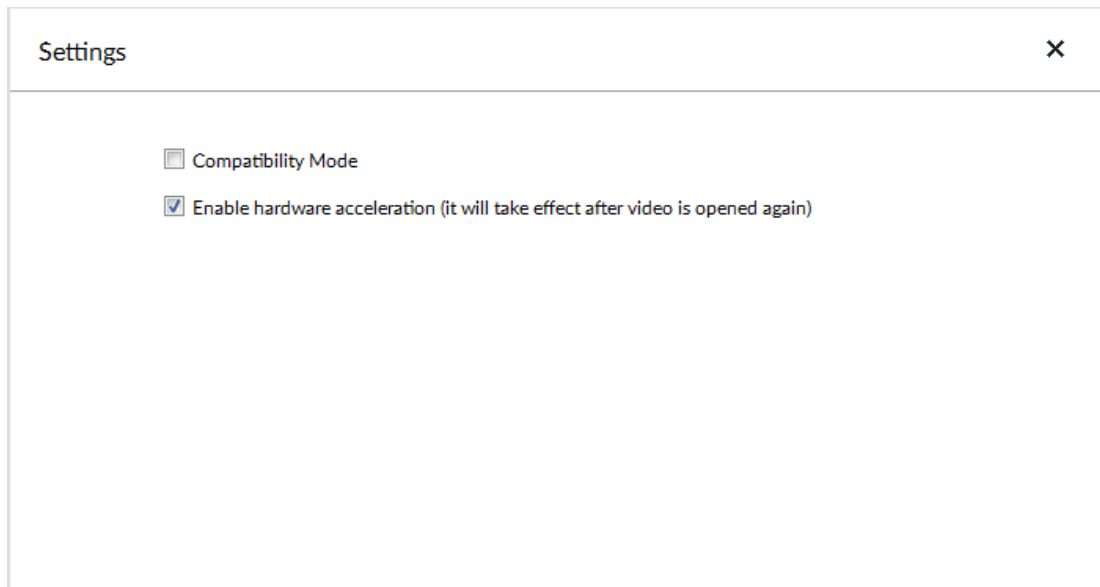
Click , and select **Settings**. The **Settings** page is displayed. Select **compatibility mode**. Restart PCAPP before the compatibility mode takes effect.

Figure 8-3 Setting




## Enabling Hardware Acceleration

Click , and select **Settings**. Select **Enable hardware acceleration (it will take effect after video is opened again)**.

The live view becomes much more fluent when this function is enabled.

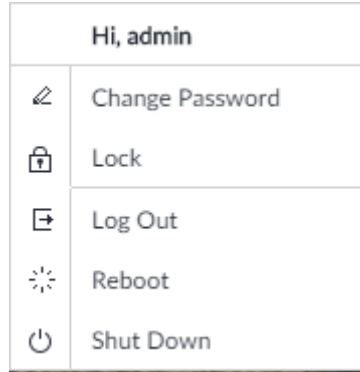
## 8.5 Viewing Version Details

Click , and then select **About** to view PCAPP version information.

# 9 Log Out, Reboot, Shut Down, Lock

Log out, reboot, shut down and lock out the Device.

Figure 9-1 User operation



## Logging Out

Click  and then select **Log Out**.


## Rebooting

Click  and then select **Reboot**. System pops up confirm dialogue box. Click **OK** to reboot.


## Shutting Down



To unplug the power cable might result in data (record and image) loss.

- Mode 1 (recommended): Click  and then select **Shutdown**. System pops up confirm dialogue box and then click **OK** to shut down.
- Mode 2: Use power on-off button on the device.
  - ◇ 8-HDD series product: Press power on-off button on rear panel.
  - ◇ Other series products: Press the power on-off button on the device for at least 4 seconds.
- Mode 3: Unplug the power cable.

## Locking


Click  and then select **Lock** to lock the client. The locked client cannot be operated.

To unlock the client, click anywhere on the client, and then the **Unlock** dialogue box is displayed. Enter the username and password, and then click **OK**. You can also click **Switch User** to switch to another user account.

Figure 9-2 Unlock the client

The image shows a dialog box titled "Unlock" with a close button (X) in the top right corner. It contains two input fields: "User Name" with a person icon and the text "admin", and "Password" with a lock icon, the text "Password", and an eye icon. At the bottom, there are three buttons: "Switch User", "OK" (highlighted in blue), and "Cancel".

# 10 FAQ

Problem	Possibilities and Solutions
<p>After enabling AI by device function, there is no human face recognition event.</p>	<p>The AI module is offline.            On the <b>LIVE</b> page, click  . Select <b>SYSTEM &gt; MAINTAIN &gt; Upgrade &gt; AI Module</b> to check the AI module is online or not.            There are too many filter criteria on the AI display page.            The registered remote device does not support face detection function.            Enable AI by device function.            It is not in the deployment period.            There is no linked face database or the face database has no data.            The human face similarity setting is too high.</p>
<p>After enabling AI by camera function, there is no human face recognition event.</p>	<p>The human face recognition function has not been enabled on the AI plan.            There is no human face database on the web page of the remote device.            It is not in the deployment period.</p>
<p>There are no human face search results.</p>	<p>The human face similarity setting is too high.            The selected remote device does not trigger the human face recognition.            There is no human face recognition on the search period            The specified human face image is not on the human face database.</p>

# Appendix 1 Mouse and Keyboard Operations

This section introduces mouse and keyboard operations.

## Appendix 1.1 Mouse Operations

Connect mouse to the USB port, you can use the mouse to control the local menu. For details, see the following table.

Operation	Description
Click (click the left mouse button)	<p>Click to select a function menu, to enter the corresponding menu page.</p> <ul style="list-style-type: none"><li>• Implement the operation indicated on the control.</li><li>• Change check box and option button status.</li><li>• Click the check box to display drop-down list.</li><li>• On virtual keyboard, select letter, symbol, English upper letter and lower letter, and Chinese characters.</li></ul>
Double-click (click the left mouse button twice)	<ul style="list-style-type: none"><li>• On the <b>LIVE</b> page, double-click one video window to zoom in the window. Click any position out of the window, so the video window restores original size.</li><li>• On the <b>LIVE</b> page, double-click the remote device in the device tree. Switch to video edit status, and add remote device.</li><li>• Double-click the image or record file thumbnail, to playback record file or view the image.</li></ul>
Right-click (click the right mouse button)	<ul style="list-style-type: none"><li>• On the <b>LIVE</b> or <b>SEARCH</b> page, right-click one video window to display the shortcut menu.</li><li>• On the <b>LIVE</b> page, right-click the view in the list or the remote device in the device tree, to display the shortcut menu.</li></ul>
Wheel button	<ul style="list-style-type: none"><li>• On the <b>SEARCH</b> page, move the mouse pointer to the time bar, and then click the mouse wheel, to adjust the accurate time on the time bar.</li><li>• Click the control that needs to input number (such as input date or time). Roll the mouse wheel to adjust the number value.</li></ul>
Drag the mouse	<ul style="list-style-type: none"><li>• Drag the mouse pointer to select the motion detect zone.</li><li>• On the <b>LIVE</b> page, drag the remote device in the device tree to the play window, switch to the view status. It is to add the remote device.</li><li>• On the <b>SEARCH</b> page, drag the record file or the image thumbnail to the playback window. It is to play back the corresponding record file or image.</li></ul>

## Appendix 1.2 Virtual Keyboard

The local menu supports virtual keyboard.

Click the text box to display virtual keyboard. For details, see the following pictures and table.





If the device has connected to the peripheral keyboard, click the text column. Virtual keyboard will disappear.

Appendix Figure 1-1 Virtual keyboard (global keyboard)



Appendix Figure 1-2 Virtual keyboard (digital keyboard)



Appendix Table 1-1 Virtual keyboard icon

Signal Words	Description
	Click the icon to switch to upper case. The icon becomes . Click  to switch to lower case.
	Click to delete letter.
	Click to input letter. Now the icon turns into . Click  to restore previous input mode.
	Click to input space.
	Click to control cursor position.
	Click to switch to the next line.
	Select text and click the icon to cut the selected contents.
	Select text and click the icon to copy the selected contents.
	Cut or copy the contents, click the text box and click the icon to paste the contents.

Appendix Figure 1-3 Virtual keyboard (input letter)



## Appendix 2 RAID

RAID is an abbreviation for Redundant Array of Independent Disks. It is to combine several independent HDDs (physical HDD) to form a HDD group (logic HDD).

Comparing with one HDD, RAID provides more storage capacity and data redundancy. The different redundant arrays have different RAID level. Each RAID level has its own data protection, data availability and performance degree.

### RAID Level

RAID Level	Description	Min. HDD Needed
RAID0	RAID 0 is called striping. RAID 0 is to save the continued data fragmentation on several HDDs. It can process the read and write at the same time, so its read/write speed is N (N refers to the HDD amount of the RAID 0) times as many as one HDD. RAID 0 does not have data redundant, so one HDD damage might result in data loss that cannot be restored.	2
RAID1	It is also called mirror or mirroring. RAID 1 data is written to two HDDs equally, which guarantee the system reliability and can be repaired. RAID 1 read speed is almost close to the total volume of all HDDs. The write speed is limited by the slowest HDD. At the same time, the RAID 1 has the lowest HDD usage rate. It is only 50%.	
RAID5	RAID5 is to save the data and the corresponding odd/even verification information to each HDD of the RAID5 group and save the verification information and corresponding data to different HDDs. When one HDD of the RAID5 is damaged, system can use the rest data and corresponding verification information to restore the damaged data. It does not affect data integrity.	3

RAID Level	Description	Min. HDD Needed
RAID6	Based on the RAID5, RAID6 adds one odd/even verification HDD. The two independent odd/even systems adopt different algorithm, the data reliability is very high. Even two HDDs are broken at the same time, there is no data loss risk. Comparing to RAID5, the RAID6 needs to allocate larger HDD space for odd/even verification information, so its read/write is even worse.	4
RAID10	RAID 10 is a combination of the RAID 1 and RAID 0. It uses the extra high speed efficient of the RAID 0 and high data protection and restores capability of the RAID 1. It has high read/write performance and security. However, the RAID 10 HDD usage efficiency is as low as RAID 1.	
RAID50	RAID50 is a combination of the RAID5 and RAID0. It has higher fault-tolerance. There is no data loss even one HDD in the set malfunctions.	6
RAID60	RAID60 is a combination of the RAID6 and RAID0. It has higher fault-tolerance and read performance. There is no data loss even two HDDs in one set malfunctions.	8

## RAID Capacity

See the sheet for RAID space information.

Capacity N refers to the mini HDD amount to create the corresponding RAID.

RAID Level	Total Space of the N HDD
RAID0	The total amount of current RAID group
RAID1	Min (capacity N)
RAID5	$(N-1) \times \text{min (capacity N)}$
RAID6	$(N-2) \times \text{min (capacity N)}$
RAID10	$(N/2) \times \text{min (capacity N)}$
RAID50	$(N-2) \times \text{min (capacity N)}$
RAID60	$(N-4) \times \text{min (capacity N)}$

## Appendix 3 HDD Capacity Calculation

HDD capacity calculation formula:

Total capacity (M) = Channel number × Demand time length (hour) × HDD capacity occupied per hour (M/hour)

According to the above formula, get recording time calculation formula.

Recording time (hour) =

$$\frac{\text{Total capacity (M)}}{\text{HDD capacity occupied per hour (M/hour)} \times \text{Channel number}}$$

For example, for single-channel recording, HDD capacity occupied per hour is 200 M/hour. Use 4-channel device to make 24-hour continuous recording in every day of one month (30 days), the required HDD space is: 4 channels × 30 days × 24 hours × 200 M/hour = 576 G. Therefore, five 120 G HDD or four 160 G HDD shall be installed.

According to the above formula, at different stream values, recording file size of 1 channel in 1 hour is shown as follows (for your reference):

Bit stream Size (max.)	File Size	Bit Stream Size (max.)	File Size
≤ 96 K	42 M	128 K	56 M
160 K	70 M	192 K	84 M
224 K	98 M	256 K	112 M
320 K	140 M	384 K	168 M
448 K	196 M	512 K	225 M
640 K	281 M	768 K	337 M
896 K	393 M	1024 K	450 M
1280 K	562 M	1536 K	675 M
1792 K	787 M	2048 K	900 M

## Appendix 4 Glossary

Name	Description
CGI	Common Gateway Interface (CGI) is an important Internet technology. With CGI, client can ask data from program running on network server. CGI describes data transmission standard between server and asking processing program.
DDNS	Dynamic Domain Name System (DDNS) is to map the user dynamic IP address to a specified domain analysis service. Each time, when the user connects to the network, the client can transmit the host dynamic address to the server application on the host of the service provider. The server applications are to provide the DNS service and realize dynamic domain analysis. That is to say, the user does not need to remember the changeable IP address, just uses the domain name to login the device or the address.
DHCP	Dynamic Host Configuration Protocol (DHCP) is a network protocol in the LAN. It is to automatically allocate IP address for the internal network or the ISP (Internet service provider).It is to manage the computer IP address by the unified means of management.
DNS	Domain Name System (DNS) is to save the all host domain name and corresponding IP address in the network. It has the ability to change the domain to the IP address.
DVR	Digital Video Recorder.
FTP	File Transfer Protocol (FTP) is used to control bilateral transmission of file on the Internet.
HDMI	High Definition Multimedia Interface (HDMI) is a special digital interface suitable for audio/video transmission. It can transmit audio signal and video signal at the same time.
HTTPS	Hyper Text Transfer Protocol over Secure Socket Layer (HTTPS) is a HTTP channel for security purpose. The HTTPS has defines the browser the world wide web service safety communication rule. It adopts encryption technology to guaranty safety access to the webpage.
IP	Internet Protocol.
IPC	IP Camera.
NTP	Network Time Protocol (NTP) is a protocol to synchronize computer time. It adopts wireless network protocol UDP, so that the computer time synchronizes with the server or the time source. It is to provide time correction of high accuracy.
NTSC	National Television Standards Committee, American national standard television and broadcast transmission and receiving protocol. This is a television standard that television scanning beam is 525 beams, 30 frames per second, interlaced scanning, odd field first and then it is followed by even field. NTSC is used in the United States of America, Japan, and so on.
NVR	Network Video Recorder
MTU	Maximum Transmission Unit (MTU) refers to the maximum data packet amount (byte) on one layer of the communication protocol.

Name	Description
ONVIF	Open Network Video Interface Forum (ONVIF) is the defined general protocol for information exchange among the network video devices. It includes search device, real-time audio/video, metadata, information control, and so on.
PAL	Phase Alteration Line, this is a television standard that television scanning beam is 625 beams, 25 frames per second, phase alteration, odd field first and then it is followed by even field. PAL color encoding is used. PAL is used in China, Europe, and so on.
PTZ	Pan Tilt Zoom (PTZ) refers to the PTZ all-direction movement, lens zoom, and focus control.
RAID	RAID is an abbreviation for Redundant Array of Independent Disks. It is to combine several independent HDDs (physical HDD) to form a HDD group (logic HDD), to provide higher storage performance and data redundancy.
S.M.A.R.T	Self-Monitoring Analysis and Reporting Technology (S.M.A.R.T) is a technical standard to detect HDD drive status and report potential problems.
SSH	Secure Shell (SSH) is a security protocol formulated by IETF network group on the basis of application layer. SSH protocol can effectively prevent information leakage problem during remote management.
SVC	Scalable Video Coding (SVC) is a video encoding technology. It can split the video streams to one basic layer and several enhanced layers according to the requirements. The basic layer provides the general video quality, frame rate and resolution, and the enhanced layer is to perfect the video quality.
VGA	Video Graphics Array (VGA) is a video transmission standard. It has high resolution, high display speed and abundant colors.
WLAN	Wireless Local Area Networks (WLAN) adopts radio frequency to realize data transmission.

# Appendix 5 Particulate and Gaseous Contamination Specifications

## Appendix 5.1 Particulate Contamination Specifications

The following table defines the limitations of the particulate contamination in the operating environment of the device. If the level of particulate contamination exceeds the specified limitations and result in device damage or failure, you need to rectify the environmental conditions.

Appendix Table 5-1 Appendix Table 1-1 Particulate contamination specifications

Particulate contamination	Specifications
Air filtration	Class 8 as defined by ISO 14644-1.
Conductive dust	Air must be free of conductive dust, zinc whiskers, or other conductive particles.
Corrosive dust	Air must be free of corrosive dust. Residual dust present in the air must have a deliquescent point less than 60% relative humidity.

Appendix Table 5-2 ISO 14644-1 cleanroom classification

Class	Maximum particles/m <sup>3</sup>					
	≥ 0.1 μm	≥ 0.2 μm	≥ 0.3 μm	≥ 0.5 μm	≥ 1 μm	≥ 5 μm
—	—	—	—	—	—	—
Class 1	10	2	—	—	—	—
Class 2	100	24	10	4	—	—
Class 3	1000	237	102	35	8	—7
Class 4	10000	2370	1020	352	83	—
Class 5	100000	23700	10200	3520	832	29
Class 6	1000000	237000	102000	35200	8320	293
Class 7	—	—	—	352000	83200	2930
Class 8	—	—	—	3520000	832000	29300
Class 9	—	—	—	—	8320000	293000

## Appendix 5.2 Gaseous Contamination Specifications

Usually indoor and outdoor atmospheric environments contain a small amount of common corrosive gas pollutants. When these mixed or single corrosive gas pollutants react with other environmental factors such as temperature or relative humidity in the long term, the device might suffer from a risk of corrosion and failure. The following table defines the limitations of the gaseous contamination in the operating environment of the device.



Appendix Table 5-3 Gaseous contamination specifications

Gaseous contamination	Specifications
Copper coupon corrosion rate	< 300 Å/month per Class G1 as defined by ANSI/ISA71.04-2013
Silver coupon corrosion rate	< 200 Å/month per Class G1 as defined by ANSI/ISA71.04-2013

Appendix Table 5-4 Appendix Table 1-4 ANSI/ISA-71.04-2013 classification of reactive environments

Class	Copper Reactivity	Silver Reactivity	Description
G1 (mild)	< 300 Å/month	< 200 Å/month	Corrosion is not a factor in determining equipment reliability.
G2 (moderate)	< 1000 Å/month	< 1000 Å/month	Corrosion effects are measurable and corrosion might be a factor.
G3 (harsh)	< 2000 Å/month	< 2000 Å/month	High probability that corrosive attack will occur.
GX (severe)	≥ 2000 Å/month	≥ 2000 Å/month	Only specially designed and packaged devices are expected to survive.

# Appendix 6 Cybersecurity Recommendations

## **Mandatory actions to be taken for basic device network security:**

### **1. Use Strong Passwords**

Please refer to the following suggestions to set passwords:

- The length should not be less than 8 characters;
- Include at least two types of characters; character types include upper and lower case letters, numbers and symbols;
- Do not contain the account name or the account name in reverse order;
- Do not use continuous characters, such as 123, abc, etc.;
- Do not use overlapped characters, such as 111, aaa, etc.;

### **2. Update Firmware and Client Software in Time**

- According to the standard procedure in Tech-industry, we recommend to keep your device (such as NVR, DVR, IP camera, etc.) firmware up-to-date to ensure the system is equipped with the latest security patches and fixes. When the device is connected to the public network, it is recommended to enable the "auto-check for updates" function to obtain timely information of firmware updates released by the manufacturer.
- We suggest that you download and use the latest version of client software.

## **"Nice to have" recommendations to improve your device network security:**

### **1. Physical Protection**

We suggest that you perform physical protection to device, especially storage devices. For example, place the device in a special computer room and cabinet, and implement well-done access control permission and key management to prevent unauthorized personnel from carrying out physical contacts such as damaging hardware, unauthorized connection of removable device (such as USB flash disk, serial port), etc.

### **2. Change Passwords Regularly**

We suggest that you change passwords regularly to reduce the risk of being guessed or cracked.

### **3. Set and Update Passwords Reset Information Timely**

The device supports password reset function. Please set up related information for password reset in time, including the end user's mailbox and password protection questions. If the information changes, please modify it in time. When setting password protection questions, it is suggested not to use those that can be easily guessed.

### **4. Enable Account Lock**

The account lock feature is enabled by default, and we recommend you to keep it on to guarantee the account security. If an attacker attempts to log in with the wrong password several times, the corresponding account and the source IP address will be locked.

### **5. Change Default HTTP and Other Service Ports**

We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.

### **6. Enable HTTPS**

We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.

### **7. MAC Address Binding**

We recommend you to bind the IP and MAC address of the gateway to the device, thus reducing the risk of ARP spoofing.

#### **8. Assign Accounts and Privileges Reasonably**

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

#### **9. Disable Unnecessary Services and Choose Secure Modes**

If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.

If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

- SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up strong passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up strong passwords.

#### **10. Audio and Video Encrypted Transmission**

If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.

Reminder: encrypted transmission will cause some loss in transmission efficiency.

#### **11. Secure Auditing**

- Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
- Check device log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.

#### **12. Network Log**

Due to the limited storage capacity of the device, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

#### **13. Construct a Safe Network Environment**

In order to better ensure the safety of device and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.