User Manual

AS1700

Date: July 2021

Doc Version: 1.0

English

Thank you for choosing our product. Please read the instructions carefully before operation. Follow these instructions to ensure that the product is functioning properly. The images shown in this manual are for illustrative purposes only.

For further details, please visit our Company's website www.zkteco.com.

Trademark

ZKTeco is a registered trademark of ZKTeco. Other trademarks involved in this manual are owned by their respective owners.

Disclaimer

This manual contains information on the operation and maintenance of the ZKTeco equipment. The copyright in all the documents, drawings, etc. in relation to the ZKTeco supplied equipment vests in and is the property of ZKTeco. The contents hereof should not be used or shared by the receiver with any third party without express written permission of ZKTeco.

The contents of this manual must be read as a whole before starting the operation and maintenance of the supplied equipment. If any of the content(s) of the manual seems unclear or incomplete, please contact ZKTeco before starting the operation and maintenance of the said equipment.

It is an essential pre-requisite for the satisfactory operation and maintenance that the operating and maintenance personnel are fully familiar with the design and that the said personnel have received thorough training in operating and maintaining the machine/unit/equipment. It is further essential for the safe operation of the machine/unit/equipment that personnel have read, understood and followed the safety instructions contained in the manual.

In case of any conflict between terms and conditions of this manual and the contract specifications, drawings, instruction sheets or any other contract-related documents, the contract conditions/documents shall prevail. The contract specific conditions/documents shall apply in priority.

ZKTeco offers no warranty, guarantee or representation regarding the completeness of any information contained in this manual or any of the amendments made thereto. ZKTeco does not extend the warranty of any kind, including, without limitation, any warranty of design, merchantability or fitness for a particular purpose.

ZKTeco does not assume responsibility for any errors or omissions in the information or documents which are referenced by or linked to this manual. The entire risk as to the results and performance obtained from using the information is assumed by the user.

ZKTeco in no event shall be liable to the user or any third party for any incidental, consequential, indirect, special, or exemplary damages, including, without limitation, loss of business, loss of profits, business interruption, loss of business information or any pecuniary loss, arising out of, in connection with, or

relating to the use of the information contained in or referenced by this manual, even if ZKTeco has been advised of the possibility of such damages.

This manual and the information contained therein may include technical, other inaccuracies or typographical errors. ZKTeco periodically changes the information herein which will be incorporated into new additions/amendments to the manual. ZKTeco reserves the right to add, delete, amend or modify the information contained in the manual from time to time in the form of circulars, letters, notes, etc. for better operation and safety of the machine/unit/equipment. The said additions or amendments are meant for improvement /better operations of the machine/unit/equipment and such amendments shall not give any right to claim any compensation or damages under any circumstances.

ZKTeco shall in no way be responsible (i) in case the machine/unit/equipment malfunctions due to any non-compliance of the instructions contained in this manual (ii) in case of operation of the machine/unit/equipment beyond the rate limits (iii) in case of operation of the machine and equipment in conditions different from the prescribed conditions of the manual.

The product will be updated from time to time without prior notice. The latest operation procedures and relevant documents are available on http://www.zkteco.com

If there is any issue related to the product, please contact us.

ZKTeco Headquarters

Address ZKTeco Industrial Park, No. 32, Industrial Road,
Tangxia Town, Dongguan, China.

Phone +86 769 - 82109991

Fax +86 755 - 89602394

For business related queries, please write to us at: sales@zkteco.com.

To know more about our global branches, visit www.zkteco.com.

About the Company

ZKTeco is one of the world's largest manufacturer of RFID and Biometric (Fingerprint, Facial, Finger-vein) readers. Product offerings include Access Control readers and panels, Near & Far-range Facial Recognition Cameras, Elevator/floor access controllers, Turnstiles, License Plate Recognition (LPR) gate controllers and Consumer products including battery-operated fingerprint and face-reader Door Locks. Our security solutions are multi-lingual and localized in over 18 different languages. At the ZKTeco state-of-the-art 700,000 square foot ISO9001-certified manufacturing facility, we control manufacturing, product design, component assembly, and logistics/shipping, all under one roof.

The founders of ZKTeco have been determined for independent research and development of biometric verification procedures and the productization of biometric verification SDK, which was initially widely applied in PC security and identity authentication fields. With the continuous enhancement of the development and plenty of market applications, the team has gradually constructed an identity authentication ecosystem and smart security ecosystem, which are based on biometric verification techniques. With years of experience in the industrialization of biometric verifications, ZKTeco was officially established in 2007 and now has been one of the globally leading enterprises in the biometric verification industry owning various patents and being selected as the National High-tech Enterprise for 6 consecutive years. Its products are protected by intellectual property rights.

About the Manual

This manual introduces the operations of **AS1700**.

All figures displayed are for illustration purposes only. Figures in this manual may not be exactly consistent with the actual products.

Document Conventions

Conventions used in this manual are listed below:

GUI Conventions

For Software	
Convention	**Description**
Bold font	Used to identify software interface names e.g., **OK**, **Confirm**, **Cancel**.
>	Multi-level menus are separated by these brackets. For example, File > Create > Folder.
For Device	
Convention	**Description**
< >	Button or key names for devices. For example, press <OK>.
[ ]	Window names, menu items, data table, and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forwarding slashes. For example, [File/Create/Folder].

Symbols

Convention	Description
	This implies about the notice or pays attention to, in the manual.
	The general information which helps in performing the operations faster.
	The information which is significant.
	Care taken to avoid danger or mistakes.
	The statement or event that warns of something or that serves as a cautionary example.

Table of Contents

1 Overview

1.1 Introduction

AS1700 is the industry's first Ascend-powered micro intelligent video platform. It adopts an intelligent platform architecture that integrates storage, compute, and search. It is a small-sized box-type device that can face edge application scenarios such as campuses, primary/ secondary education, communities, and small stores. It features superior computing performance, user-friendly local display unit (hereinafter the LDU) design, device plug-and-play, easy management and O&M, and high reliability.

Features

High Performance and Flexible Applications

- Supports a maximum of 64-channel network video access and 320 Mbit/s video input.
- Supports all-channel image-based intelligent analysis for a maximum of 64 channels.
- Supports concurrent execution of up to six algorithms for:

  Video- and image-based facial analysis, object classification, and behavior analysis.
- Supports hybrid storage of video and images.
- Supports the algorithm repository and allows users to load and manage algorithms as plug-ins.
- Supports single-node deployment, multi-node deployment, and multi-level synergy with the IVS3800.
- Supports connections to the public cloud.

High Reliability

- Supports SafeVideo+ technology, ensuring that data is still readable and writable in remaining normal disks even if there is a RAID5 failure.
- Supports video buffering technology, ensuring video data integrity.
- Supports recording lock, preventing important recordings from being overwritten within a specified period.
- Supports the Data Safe function, enabling dual backup of key system data.

Multiple Intelligent Analysis Functions

- Supports intelligent synergy with cameras.
  - The metadata obtained by camera intelligent analysis can be directly stored in the AS1700 for subsequent intelligent services.
  - Behavior alarms generated by cameras can be directly reported to the AS1700.

Easy Deployment and Maintenance

- Free of system disks and available upon device startup.
- Plug-and-play and automatic discovery of camera settings.
- Provides status indicators, facilitating device and disk maintenance.

Cloud-Edge Synergy

- Allows upper-level surveillance platforms to view video and images from the AS1700 and subscribe to analysis result metadata and alarms.
- Allows the upper-level surveillance platform to deliver a blacklist/whitelist library or static library to perform alert on the AS1700.

1.2 Appearance

Front Panel

Rear Panel

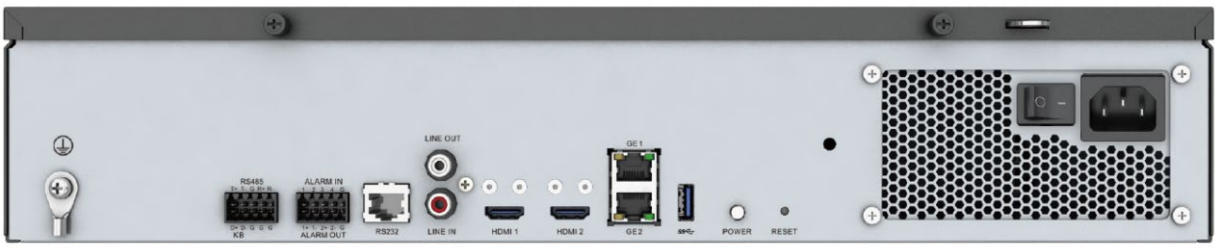


Figure 1-1 Appearance of AS1700

2 Instructions for use

2.1 Product Components

Front Panel

1. USB 2.0 port
2. GE1 network port indicator
3. GE2 network port indicator
4. Hard disk status indicator
5. Power status indicator

Figure 2-1 The ports on the front panel

Port Description:

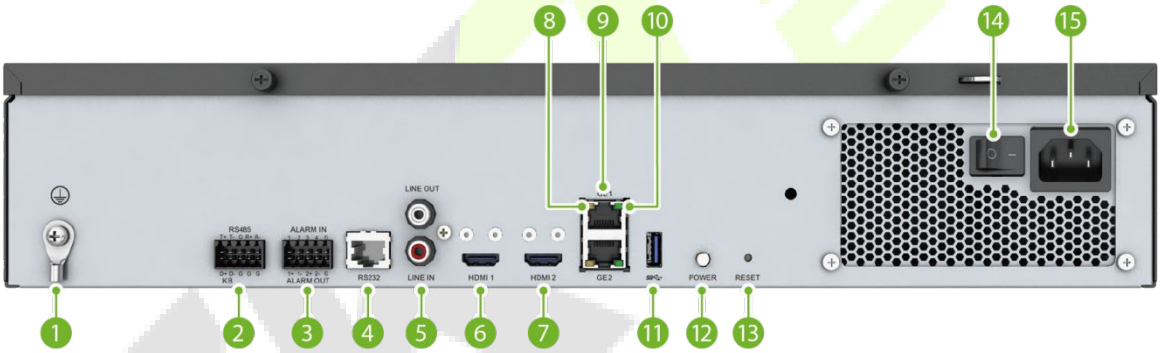
NO.	Port	Type	Function
1	**USB port**	USB2.0	Connects to one of the following USB devices: • USB flash drive • USB mouse • Removable hard disk

Indicator Description:

NO.	Indicator	Status Description
2/3	**LAN network port indicator**	Steady green: The network ports on the rear panel are properly connected. Off: The network ports on the rear panel are not properly connected.
4	**Hard disk status indicator**	Blinking green: Data is being read from or written to the hard disk. Steady red: At least one hard disk is faulty. Off: No data is being read from or written to the hard disk.

NO.	Indicator	Status Description
5	**Power indicator**	Steady green: The device is running properly. Blinking yellow at 5 Hz (on for 0.1s and off for 0.1s): A non-hard disk fault has occurred but will not affect services. Overtemperature or fan blocking occurs. Blinking red at 5 Hz (on for 0.1s and off for 0.1s): A critical fault has occurred, which will affect services. Faults include continuous high temperature, fan failure, and other component faults. Off: The device is shut down. The scenarios are as follows: • The power switch is not turned on, and the device is powered off. • The power button is not turned on, and the software is not running.

Rear Panel



1. Ground terminal
2. RS-485 port
3. Alarm input/output port
4. Serial port
5. Audio input/output port
6. HDMI 1.4 port
7. HDMI 2.0 port
8. Network port ACT indicator
9. GE network port
10. Network port LINK indicator
11. USB 3.0 port
12. Power button
13. Reset button
14. Power switch
15. Power supply port

Figure 2-2 The ports and buttons on the rear panel

Port and Button Description:

NO.	Port and Button	Type	Function
1	**Ground terminal**	-	Connects to a ground cable.
2	**RS-485 port**	RS-485	Connects to an external PTZ device or access control system. This port is reserved for hardware but not for software functions.

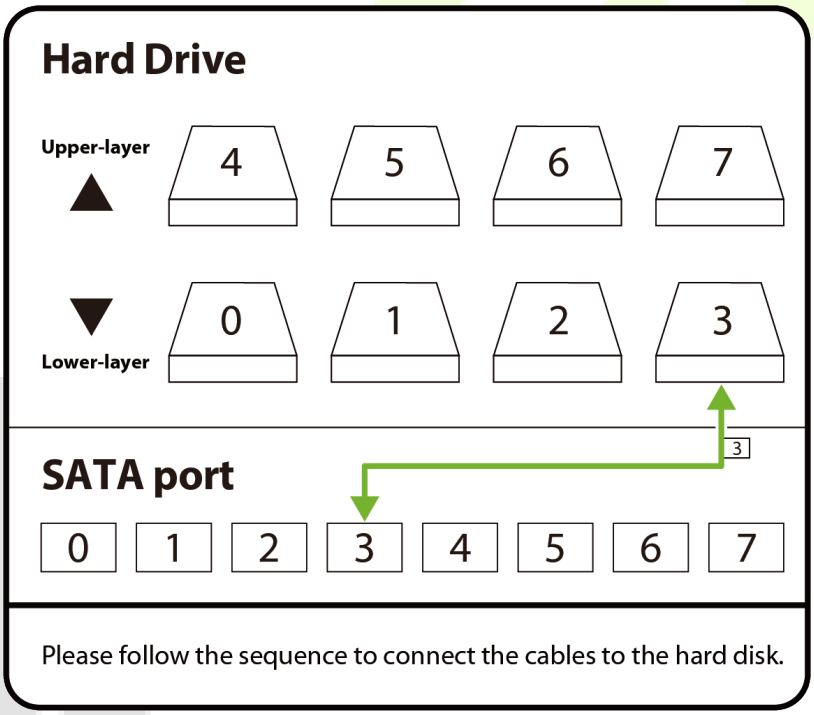
NO.	Port and Button	Type	Function
3	**Alarm input port**	IO terminal	Connects to an external alarm input device, for example, the access control system.
3	**Alarm output port**	IO terminal	Connects to an external alarm input device, for example, an alarm bell.
4	**Serial port**	COM	Used for device access and maintenance.
5	**Audio input port**	RCA	Used for audio input. This port can be used to broadcast voice files or talk with users in the surveillance area where cameras with microphones are installed.
5	**Audio output port**	RCA	Used for audio output. This port can be used to listen to channel-associated voice of cameras.
6/7	**High-Definition Multimedia Interface (HDMI) port**	HDMI	Used for HDMI video output and supports dual-HDMI output from different sources. • The HDMI 1.4 port supports a maximum resolution of 1080p. • The HDMI 2.0 port supports a maximum resolution of 4K.
9	**GE1/GE2 network port**	RJ-45	GE Ethernet port used to connect to a network cable.
11	**USB port**	USB3.0	Connects to one of the following USB devices: • USB flash drive • USB mouse • Removable hard disk
12	**Power button**	-	Used to power on or off the service software. • After the power switch of the device is turned on, the device automatically enters the running state. You do not need to press the power button. • When the power switch is turned on, you can press the power button and hold it down for 10 seconds to enter the standby mode. If you press the power button again, the device enters the running state. When the device is in standby mode, the power button indicator is steady blue. When the device is running, the power key indicator is off.
13	**Reset button**	-	• Hold down this button for 1s to reset the system. • Hold down for 10s to restore factory defaults.
14	**Power switch**	-	Used to power on or off the device.
15	**Power supply port**	-	Connects to the power supply.

Indicator Description:

NO.	Indicator	Status Description
8	**Network port ACT indicator**	Off: No data is being transmitted. Blink: Data is being transmitted.
10	**Network port link indicator**	On: The network port is properly connected. Off: The network port is not connected.
12	**Power-on/off status indicator**	On: The service software is running. Off: The service software is not started.

2.2 Wearing Instructions

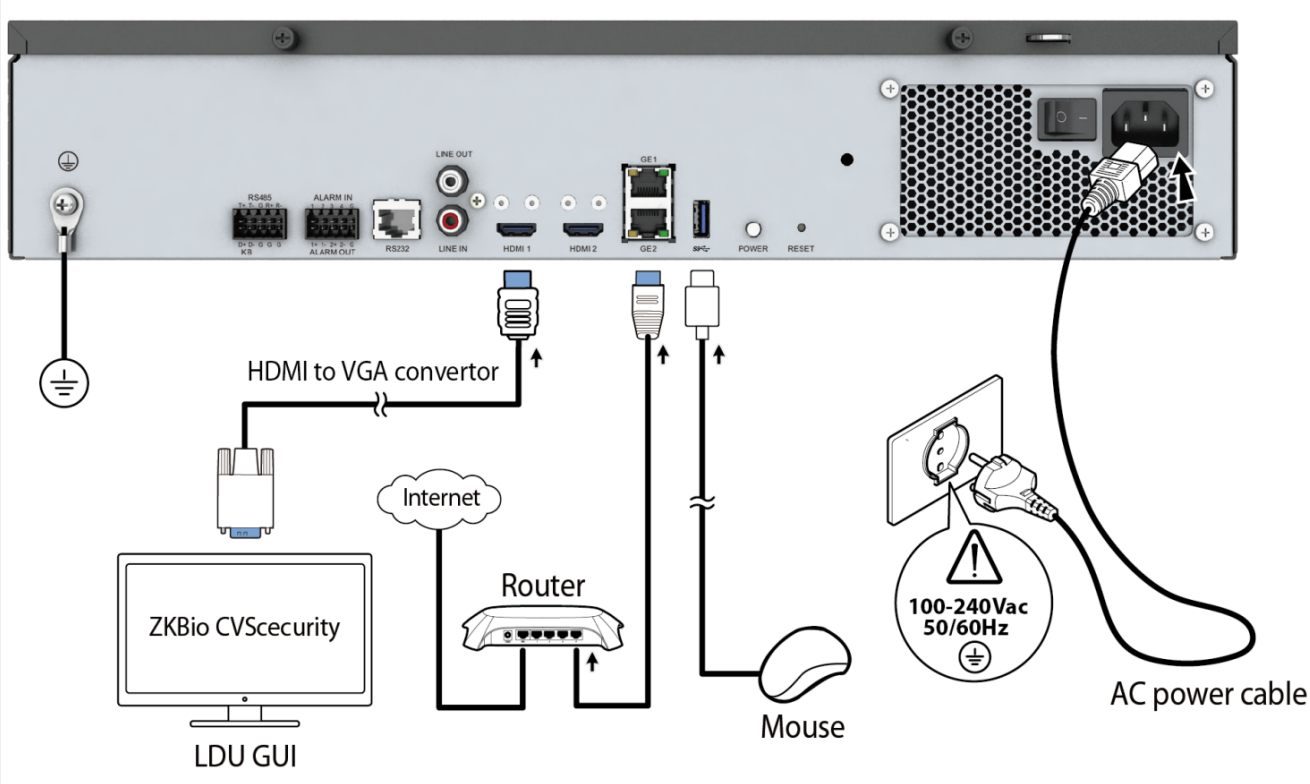
Connect the hard drive data cable and power cable



Connect the data and power cables to each hard disk in sequence from 0 to 7.

Method: Connect the SATA ports P0 to P3 to the hard disk of the lower tray, and connect the P4 to P7 ports to the hard disk of the upper tray. As shown in the figure above, connect the third hard disk to SATA port P3.

Connect the device



1. Insert the AC power cord plug into the power supply port.
2. Plug in the network cable to the GE network port. (Note: The IP address of the server (PC) and the device can be cross-segment, but it must belong to the same subnet, and the gateway and IP address must be in the same network segment when connecting to the AS1700 software.)
3. Connect a monitor to the HDMI 2.0 port to display the LDU operation interface.
4. Connect a mouse to the USB port to operate the LDU interface.
5. After powering on the device, press the power switch to start operating the device.

2.3 Package List

The package consists of the following items:

Component	Quantity	Component	Quantity
AS1700 device	1pc	Rubber feet	4pcs
AC power cable	1pc	Phoenix connectors	2pcs
Quick Start	1pc	HDMI to VGA convertor	1pc
Mounting ears	2pcs	Hard disk screws	32pcs
Mounting ear screws	8pcs	Power cable clip	1pc

2.4 Technical Parameters

This section describes only general specifications. For more advanced specifications, contact onsite product manager.

Type	Subtype	AS1700-C08016-4T
Device Performance	Network video access	16-channel 1080p, up to 160 Mbit/s access bandwidth
	Video forwarding	16-channel 1080p, up to 160 Mbit/s forwarding bandwidth
	Playback and download	16-channel 1080p, up to 80 Mbit/s playback bandwidth
Video output	HDMI	Two HDMI output interfaces: one HDMI 2.0 interface with the output resolution of 4K and one HDMI 1.4 interface with the output resolution of 1080p
	VGA	External conversion cables can be used to extend VGA ports.
	Preview mode	1/4/8/9/16
Platform performance	Cameras connected	16 cameras to one device
Controller	Processor	Hi3559A
	Memory	8 GB DDR4
Storage capacity	Disk quantity	8
	Disk interface	SATA3.0
	Disk type	
Recording management	Recording mode	Manual recording, scheduled recording, and alarm-triggered recording
	Recording playback	Multi-channel playback and segment-based playback

Type	Subtype	AS1700-C08016-4T
Compatibility	Video format	H.264, H.265, and MJPEG
	Device access	ZKTeco SDK, GB/T 28181, and ONVIF standards
	Platform access	Platform connection through GB/T 28181 (Chinese standard) or ONVIF for services such as live video viewing and PTZ controls (only for NVRs)
Intelligent analysis	Video-based object classification	2-channel 1080p or 1-channel 4K
	Video-based facial analysis	4-channel 1080p or 1-channel 4K
	Image-based facial analysis	16-channel 1080p or 12-channel 4K
	Behavior analysis	2-channel 1080p or 1-channel 4K Behavior analysis, including tripwire crossing, intrusion, area entry, area exit, loitering, and fast movement detection
	Hybrid mode	• 4-channel 1080p video-based facial analysis • 2-channel video-based facial analysis = 1-channel video-based object classification = 1-channel behavior analysis = 6-channel image-based facial analysis
Intelligent search	Face list quantity	32
	Total face list quantity	300,000
	Vehicle list quantity	5
	Total vehicle list quantity	50,000
External ports	Network ports	2 x 10/100/1000M Ethernet port
	USB port	3 USB ports (2 USB 2.0 ports on the front panel and 1 USB 3.0 port on the rear panel)
	Audio input	1 channel, RCA connector
	Audio output	1 channel, RCA connector
	Alarm port	4-channel input, 2-channel output
Other specifications	Ambient temperature range	–5°C to +55°C
	Operating humidity	20% to 90%
	Power consumption (8 disks included)	124 W
	Fan	Intelligent rate control

Type	Subtype	AS1700-C08016-4T
	Power supply	110–220 V AC
	Dimensions	86 mm (H) x 442 mm (W) x 467 mm (D)
	Rack	2 U
	Weight (hard disks excluded)	6.60 Kg
Authentication information	China	Type inspection report issued by the Ministry of Public Security of China, GB/T 28181 certification, CCC, and CQC
	Countries/Regions outside China	RoHS, REACH, WEEE, CE, CB, and UL certificate issued by four countries from the Middle East (Uganda, Kuwait, Nigeria, and Algeria)

3 LDU

The LDU scenario is suitable for the scenario where a single device is deployed. In this configuration scenario, there is no need to prepare a PC, only a monitor.

3.1 LDU Networking Scenario

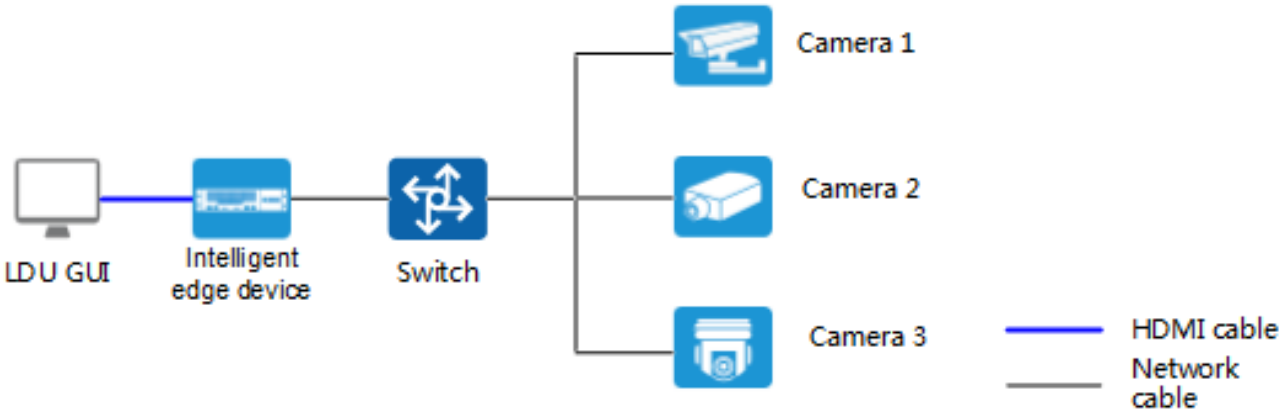


Figure 3-1 LDU networking

Application Limitations

The LDU output resolution can be 1440 x 900 pixels or 1920 x 1080 pixels. The default resolution is 1920 x 1080 pixels. Ensure that the resolution of the monitor is greater than or equal to 1920 x 1080 pixels.

3.2 Configuring the Startup Wizard

When you logs in to the LDU for the first time, the system enters the startup wizard interface. Please refer to the following steps to complete the startup wizard configuration.

3.2.1 Introduction

- The initialization navigation is displayed only when you log in to the device for the first time.
- The LDU can be connected to an external USB keyboard.
- The LDU supports the dual screens.
  - By default, the screen connected to the HDMI 2 port is the primary screen, which can be used for live video viewing and other related operations. The screen connected to the HDMI 1 port is the secondary screen, which can be used only for live video viewing.
  - The LDU supports dual-screen switching, after which the primary screen becomes the secondary screen, and the original secondary screen becomes the primary screen.

- The screen connected to the HDMI 2 port supports at most 32-channel live video while the screen connected to the HDMI 1 port supports at most 16-channel live video. The number of channels supported for live video viewing depends on only what HDMI port a screen is connected to.

3.2.2 Configuration Steps

Step1: Setting the Password

- Set the service system and operating system passwords at the first login.

1. Set the password of the **admin** user of the service system, as shown in the Figure 3-2.

Figure 3-2 To set the password of the **admin** user of the service system.

Function Description

User/Password	Description
admin	You need to customize a password for the **admin** user of the service system. • As a predefined user of the system, the **admin** user has all permissions. The role and name of the **admin** user cannot be modified.
Password/Confirm Password	• Only the **admin** user can log in to the LDU. • After the password of the **admin** user is set, the user will not be logged out of the system and can use services normally.

User/Password	Description
	NOTE: *For security purposes, it is recommended to use a password with high complexity.*

2. Set the password of the **admin** user of the operating system, as shown in the Figure 3-3.

Figure 3-3 Setting the password of the admin user of the operating system.

Function Description

User/Password	Description
admin	You need to customize a password for the **admin** user of the operating system. • The **admin** user is an operating system user and can be used to both remotely and locally log in to the operating system.
Password/Confirm Password	**NOTE:** *For security purposes, it is recommended to use a password with high complexity.*

3. Set the password of the **root** user of the operating system, as shown in the Figure 3-4.

Figure 3-4 Setting the password for the **root** user of the operating system.

Function Description

User/Password	Description
root	You need to customize a password for the **root** user of the operating system. • The **root** user has the highest permission on any file, directory, and process. • To perform operations as the **root** user, log in as the **admin** user and then switch to the **root** user, instead of directly logging in as the **root** user. **NOTE:** *For security purposes, it is recommended to use a password with high complexity.*
Password/Confirm Password	

Step2: Re-logging in

- Use the configured service system password to log in to the system again, as shown in Figure 3-5.

Figure 3-5 Re-logging in

Step3: Configuring Disk Parameters

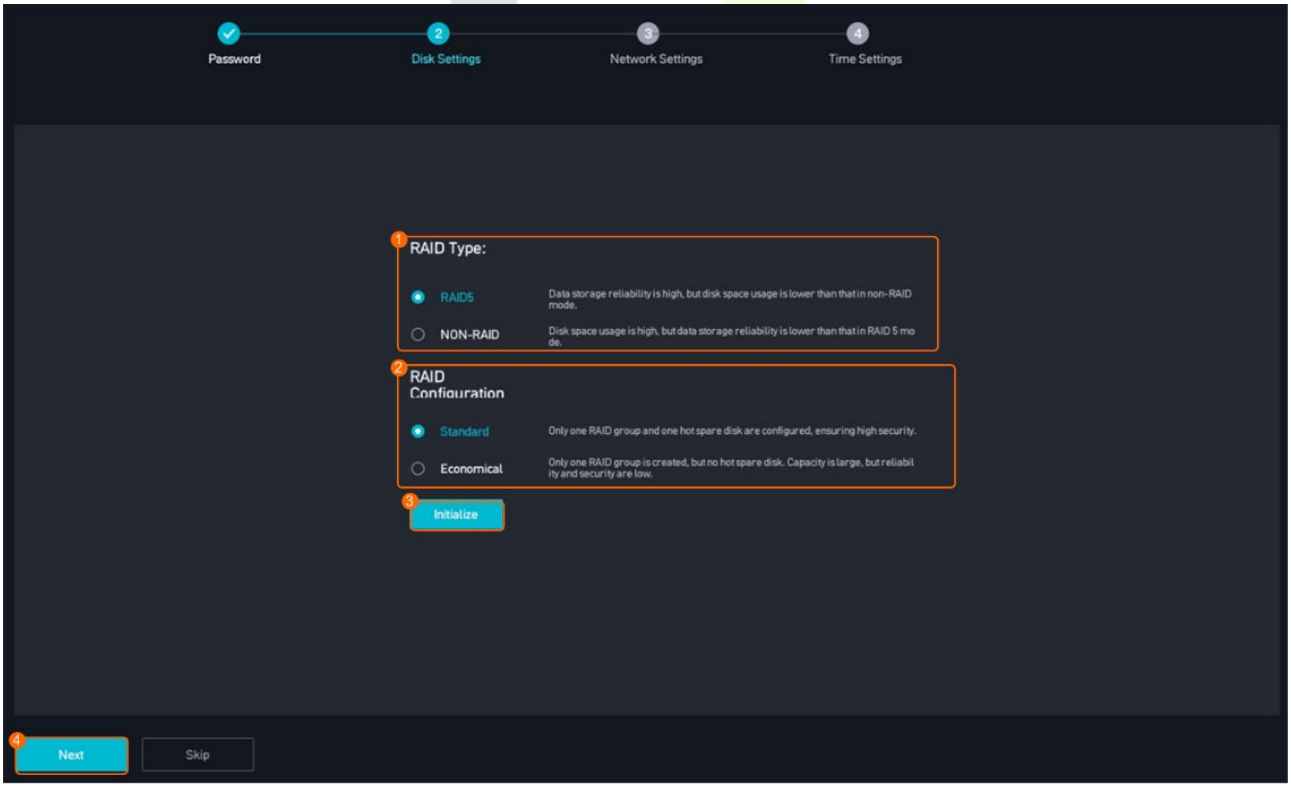


Figure 3-6 Setting disk parameters

RAID Mode Description

RAID Mode	Description
RAID 5	All hard disks form a RAID 5 group. Each recording file is stored on all hard disks. RAID 5 provides higher data storage reliability, but its disk usage is lower than that in non-RAID mode. • **Standard** – Four or more hard disks are required. – One hard disk is used as a hot spare disk. The hot spare disk does not store data. When a hard disk in the RAID group is faulty, the hot spare disk will replace the faulty one and function as a member disk of the RAID group. – Actual capacity = (Total number of disks - 2) x Minimum disk capacity One hard disk is used as the hot spare disk. To ensure that the data in the RAID group can be restored, storage space must be reserved on each hard disk. The sum of reserved space sizes is equal to the size of a hard disk. – The disk usage is lower than that in economical configuration mode, but the data storage reliability is higher than that in economical configuration mode. • **Economical** – Three or more hard disks are required. – No hot spare disk is configured. – Actual capacity = (Total number of disks - 1) x Minimum disk capacity To ensure that the data in the RAID group can be restored, storage space must be reserved on each hard disk. The sum of reserved space sizes is equal to the size of a hard disk. – The disk usage is higher than that in recommended configuration mode, but the data storage reliability is lower than that in recommended configuration mode.
NON-RAID	Each recording file is stored on only one hard disk. The disk usage is high, but the data storage reliability is lower than that in RAID 5 mode.

- Hard disks from different vendors cannot be used together.
- Different types of disks from the same vendor cannot be used together. For example, monitoring disks and enterprise disks cannot be used together.
- Hard disks of the same type from the same vendor are used together (for example, 4 TB and 6 TB enterprise disks are used together):
  - If the hard disks are configured in RAID 5 mode, the total capacity will be bound by the disk of the smallest size in the group.

    For example, if one 4 TB hard disk and two 6 TB hard disks are configured in RAID 5 economical mode, the actual available capacity is 8 TB.
  - If the hard disks are configured in non-RAID mode, the actual available capacity of each hard disk is the actual capacity of the hard disk.

    For example, if one 4 TB hard disk and two 6 TB hard disks are configured in non-RAID mode, the actual available capacity is 16 TB.

Step4: Setting Network Parameters

- **One address mode**
  - If the intelligent edge device, cameras, and surveillance client are on the same network, select the one address mode.

Set the IP address, gateway address, and subnet mask of the device based on the site requirements, as shown in Figure 3-7.

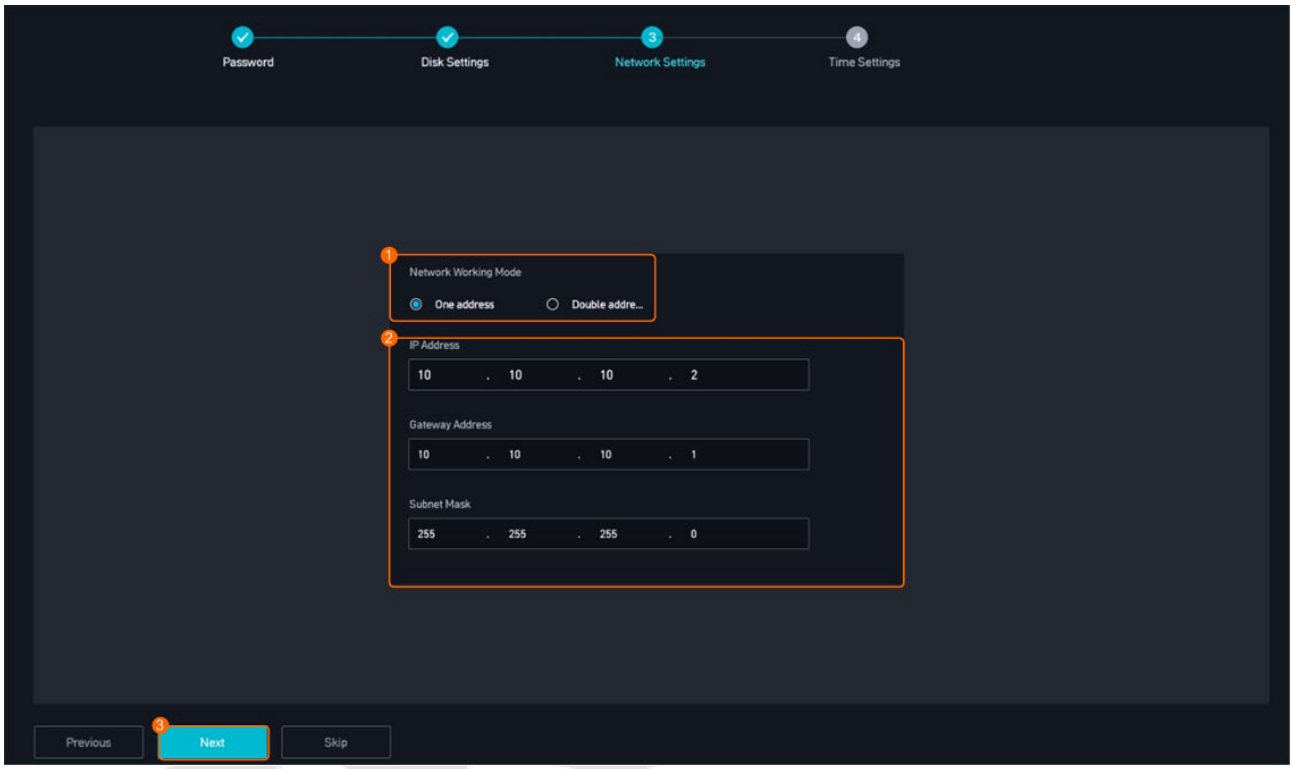


Figure 3-7 Single address mode

NOTE:

After setting the new IP address, follow the startup wizard to complete the configuration and restart the device.

- **Double address mode**
  - If the intelligent edge device, cameras, and surveillance client are on different networks, select the double address mode.
    - Cameras can be connected to the AS1700 through the GE2 network port, which is used for southbound connection.
    - The VMS is connected to the AS1700 only through the GE1 network port, which is used for northbound connection.

Set the IP addresses of GE1 (ETH1) and GE2 (ETH0) based on the actual situation, as shown in Figure 3-8.

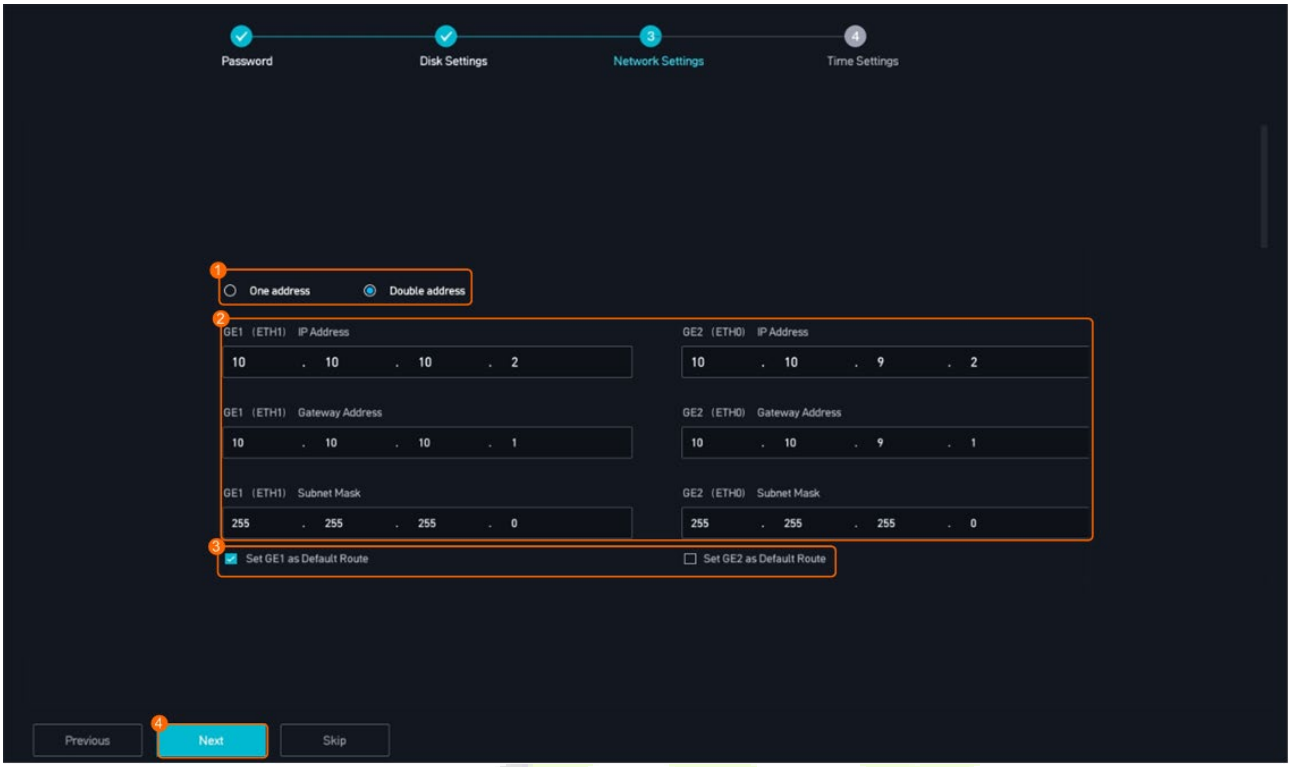


Figure 3-8 Double address mode

NOTE:

- The IP addresses of GE1 (ETH1) and GE2 (ETH0) cannot be in the same network segment.
- If the northbound platform environment is in the same network segment as ETH1, the default route can be set to any value.
- If the northbound platform and ETH1 are in different network segments, the northbound platform network must be able to communicate with the network of the current default gateway. Otherwise, the connection fails.
- After setting the new IP address, restart the device after following the startup wizard.

Step5: Configuring the Time

- If an NTP server is configured onsite, synchronize the time from the NTP server, as shown in Figure 3-9.

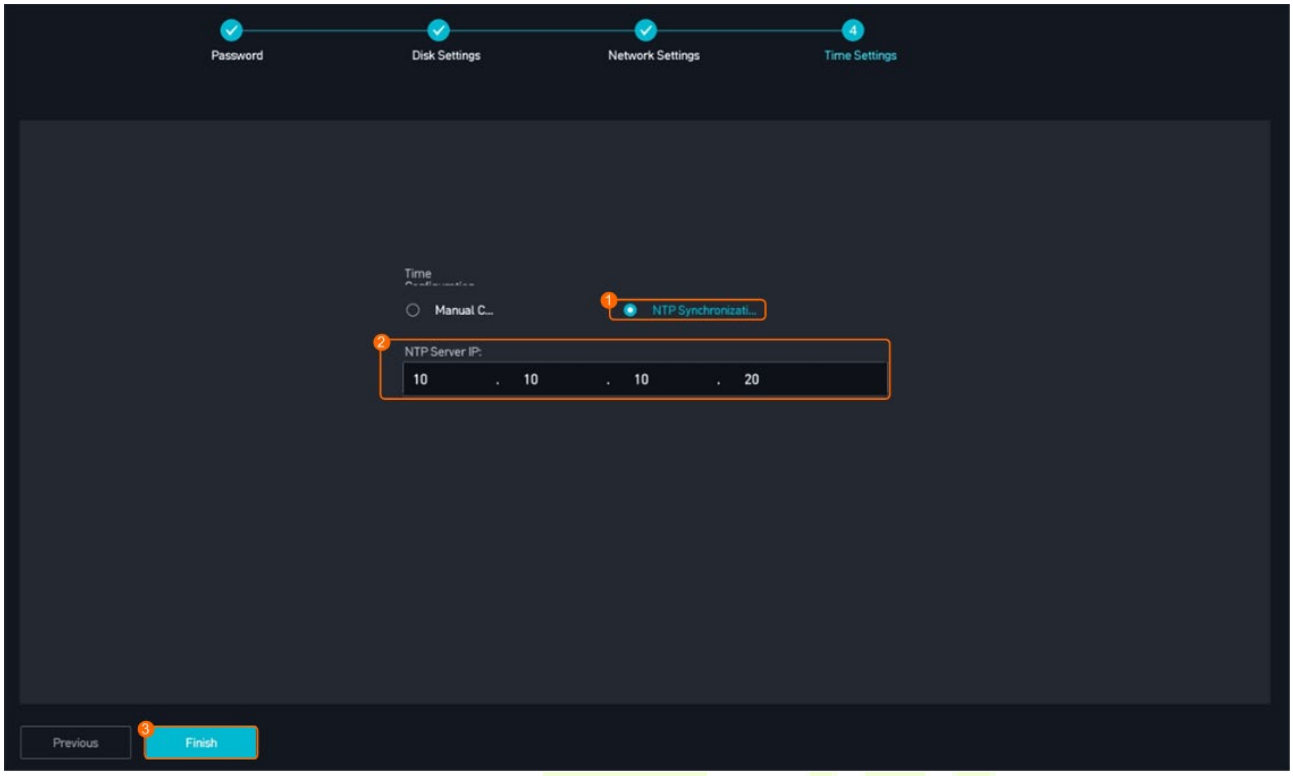


Figure 3-9 NTP time synchronization

- If no NTP server is configured onsite, manually configure the time, as shown in Figure 3-10.

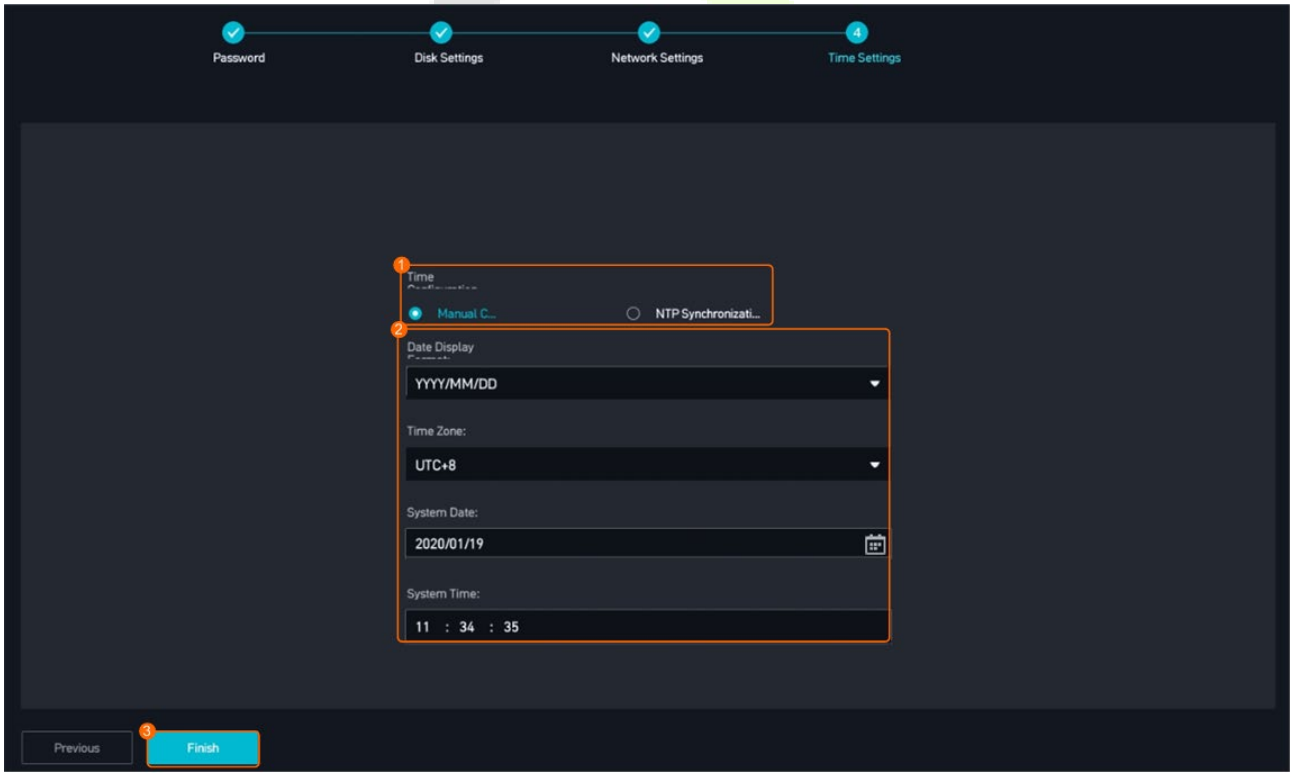


Figure 3-10 Manual time configuration

After completion, the system will automatically jump to the camera adding interface.

Step6: Adding cameras

- The device automatically searches for cameras whose IP addresses are in the same network segment. Cameras can be connected through HWSDK or ONVIF.

  For example, if the IP address of the device is 192.168.1.12, the device automatically searches for cameras whose IP addresses are in the network segment from 192.168.1.0 to 192.168.1.254.

- For details about how to connect cameras in the following scenarios, see Connecting Cameras.
  - Connecting cameras through GB/T 28181
  - Connecting cameras over a Layer 2 network

  Note: In this access scenario, ensure that the device and cameras are on the same VLAN as the switch.

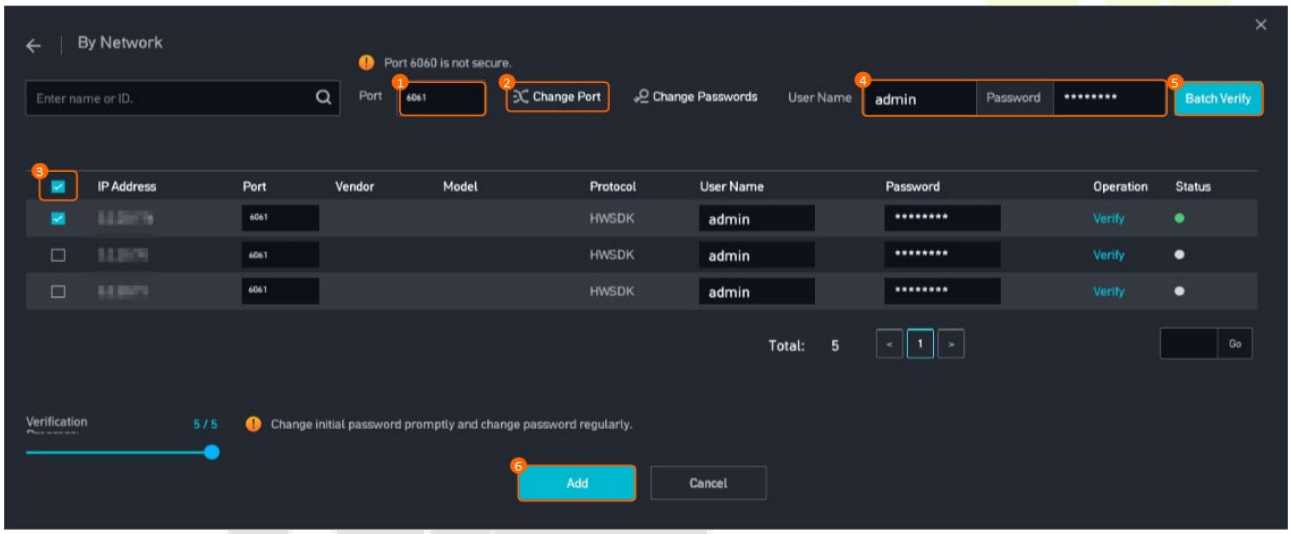


Figure 3-11 Connecting cameras by network segment

Function Description

Parameter/Button	Description	Remarks
Port	• HWSDK – If the cameras use the encryption transmission protocol TLS, set the port number to **6061**. **It takes a long time to connect cameras through port 6061.** – If the cameras use a non-encryption transmission protocol, set the port number to **6060**. Non-encryption transmission protocols may have security risks. You are advised to use an encryption transmission protocol. • ONVIF Set the port number to **80**.	• Cameras whose software version is earlier than V500R019C20 do not support port 6061. Use port 6060 for these cameras. To view the camera software version, log in to the camera web system. • If a camera fails to be connected, rectify the fault by referring to 5.8.3.1 Failure to Verify a Camera When You Follow the Wizard to Add It.

Parameter/Button	Description	Remarks
Change Port	Button for changing camera ports in batches.	-
Change Passwords	Button for changing camera passwords in batches.	-
User Name/Password	User name and password for registering a camera through the HWSDK protocol.	-
Batch Verify	Button for verifying the registration user names and passwords of cameras in batches.	If the verification is passed, is displayed. If not, is displayed.
Verify	Button for verifying the registration user name and password of a single camera.	If the user name or password of a camera has been changed after registration, the camera may fail the batch verification. You can configure the user name or password for the camera and then independently verify the camera.

3.3 Login to the LDU

- After configuring the startup wizard you can login to the LDU.
- On the Login page, enter the **admin** username and password.

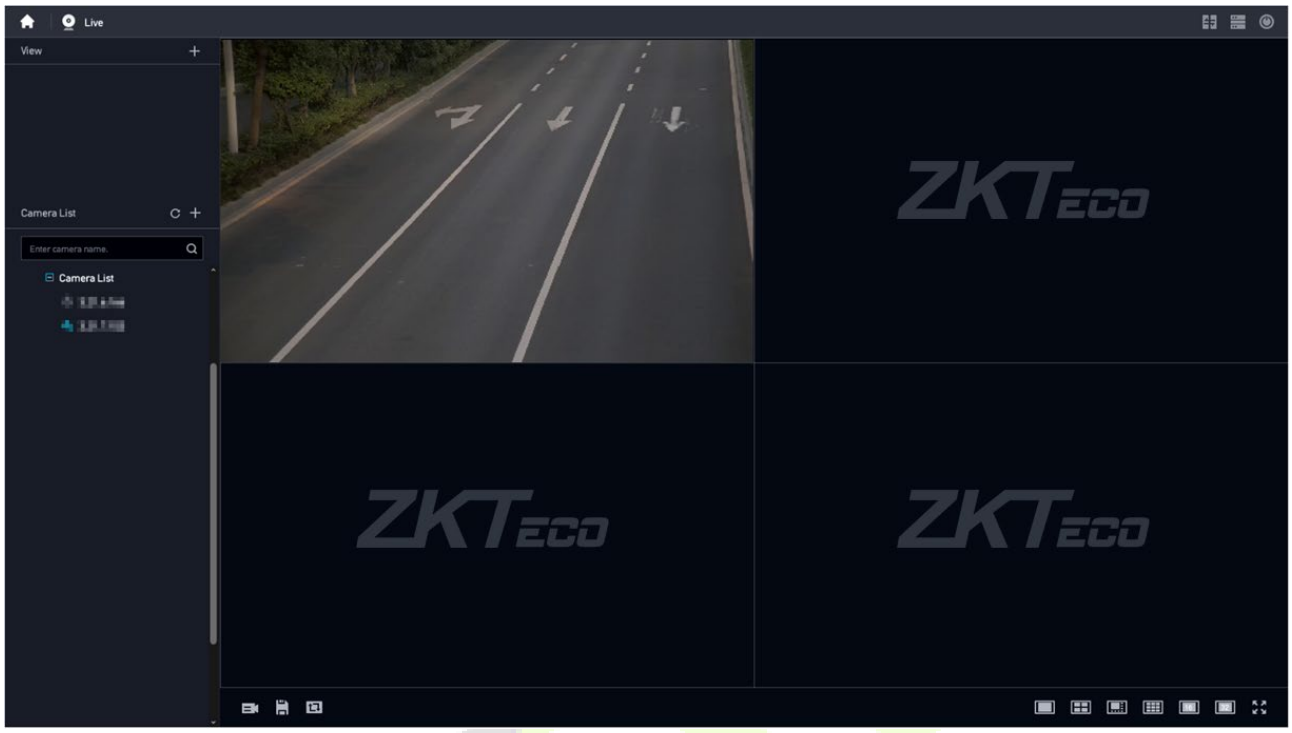
Figure 3-12 LDU login interface

NOTE:

When you log in to the LDU for the first time, the startup wizard page is displayed. Configure the

system following the startup wizard by referring to 3.2Configuring the Startup Wizard.

- After you log in to the LDU, the **Live** interface is displayed by default, as shown in below.



Checking the Device Version

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop to enter the Main Menu.

Step 3 Choose **System Management** > **System Info**.

Step 4 View the current system version.

- For V100R019C50, upgrade the version to V100R019C50SPC100 or later.
- For V100R019C50SPC100 or later, you are advised to upgrade the system version to the latest released version.
- For how to upgrade, please refer to the ***Upgrade Guide*** under the corresponding version.

NOTE:

Due to permission settings, you need to log in to view the software version.

If some software versions cannot be downloaded, please ask for technical support.

4 Operation Interface of LDU

On the **Live** interface, click button in the upper left corner or right-click on the desktop to go to the **Main Menu,** as shown in below.

4.1 Live

Users can remotely view live video shot by cameras to monitor onsite conditions in real time.

4.1.1 Configuring Real-Time Surveillance

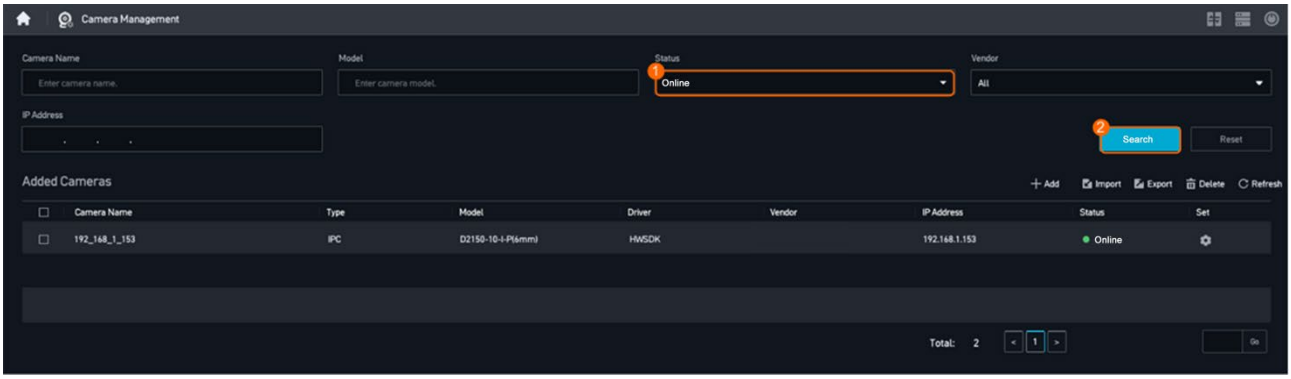
Check whether the device is online

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop to enter the Main Menu.

Step 3 Choose **Camera Management**.

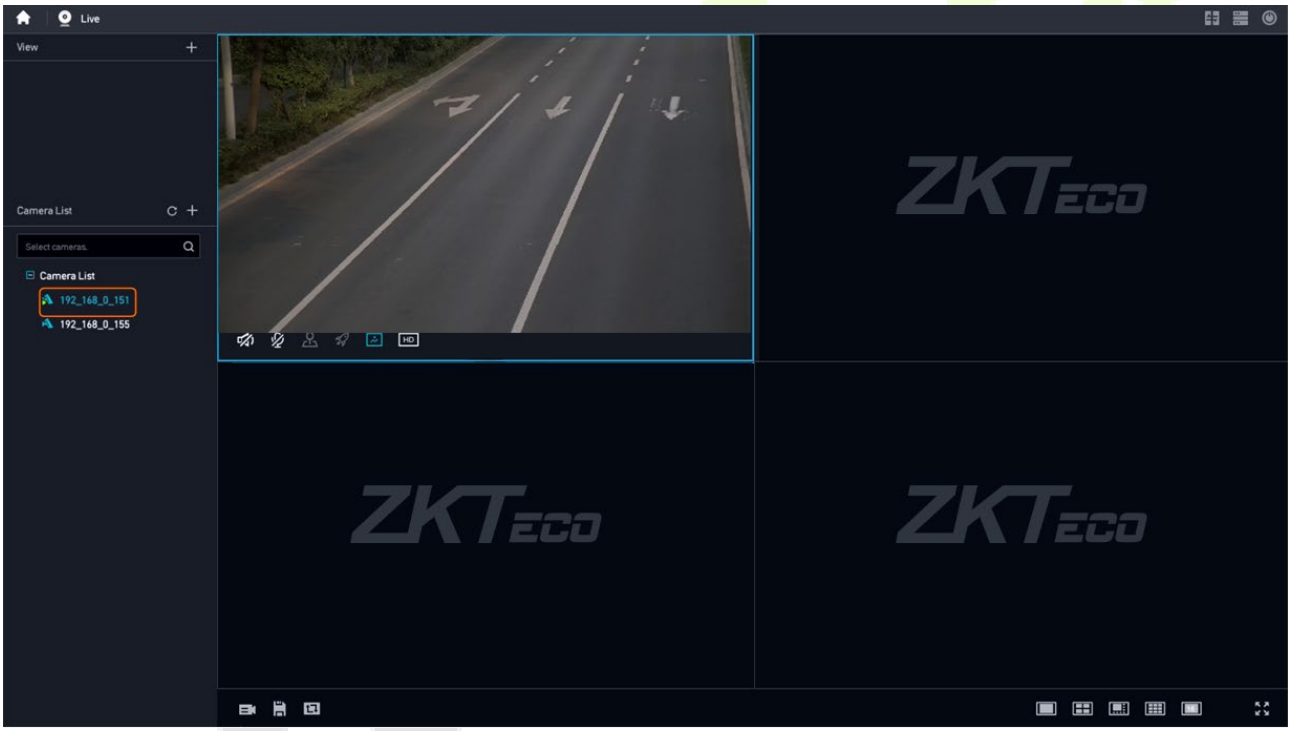
Step 4 Search for online cameras, as shown in below.



Live Video Surveillance

Step 1 Log in to the LDU as the **admin** user.

Step 2 Drag a camera from the camera list to a live video pane, as shown in below.



NOTE:

- Do not enable media security under **Camera Configuration** > **Video** > **Extended Settings**. Otherwise, a blank screen may occur during live video viewing on the LDU. (**Note:** The camera configuration can be found on the **Camera Management** interface, and click **Set** to open it.)
- In the dual-screen scenario, the monitor connected to the HDMI2 port of the AS1700 is the primary screen by default, where you can perform operations such as GUI configuration. The monitor connected to the HDMI1 port of the AS1700 is the secondary screen, where you can view live video but cannot perform operations such as GUI configuration.

- You can click  in the upper right corner of the page to switch between the primary and secondary screens. After the switchover, the original primary screen becomes the secondary screen and only supports live video viewing. The original secondary screen becomes the primary screen and supports operations such as GUI configuration.

Function Description

Icon	Function
	Switches to recording playback.
	Adds a view layout to favorites. For details, see 4.1.3Live Video View Management.
	Manages camera sequencing. For details, see 4.1.2Camera Cycling.
	Adjusts the live video pane layout.
	Enables you to hear sounds, if any, from the surveillance sites being monitored by the camera whose live video is being viewed, through audio output devices. To use this function, the camera whose live video is being viewed must support the audio function or is configured with a sound pickup device.
	Enables voice intercom. For details, see 4.1.4Voice Intercom. This function can be enabled only when the following conditions are met: • A camera supports the voice intercom function. • A microphone and a speaker are available for the camera. • A microphone and a speaker have been configured on the LDU.
	Controls the PTZ. For details, see 7.2 PTZ Controls. This function requires that the camera support PTZ controls. Otherwise, the icon is unavailable.
	Enables the network speed priority function (enabled by default). If the network bandwidth fluctuates greatly, **the function ensures video real-timeliness preferentially**, so that frame freezing may occur.
	Enables the image quality priority function. If the network bandwidth fluctuates greatly, **the function ensures video smoothness preferentially**, so that video latency may occur.
	• H264 • H265 If the image quality of the live video is poor, you can switch the stream to ensure the image quality. For details, see 4.3.9.1.2 Feature Configuration.

4.1.2 Camera Cycling

Users can play live video from multiple cameras in turn based on specified rules.

Definition

- Users can play live video from multiple cameras in turn based on specified rules.

Customer Benefits

- Cameras are automatically switched, saving the labor cost.
- Users can configure cameras in an area as a camera cycling resource to uniformly view the surveillance video of the area.
- Users can set an execution period for a camera cycling task. During this period, camera cycling is automatically executed, improving operation efficiency and facilitating task arrangement.

Application Scenario

- Users can set a camera cycling task for cameras around a warehouse to view the surroundings of the warehouse in turn.

Scenario Description

- You can configure a cycling policy to view live video from multiple cameras at a certain interval.

Prerequisites

- You have commissioned real-time surveillance by referring to 4.1.1 Configuring Real-Time Surveillance.
- You have configured preset positions by referring to 7.2.3Configuring Preset Positions and the Home Position.

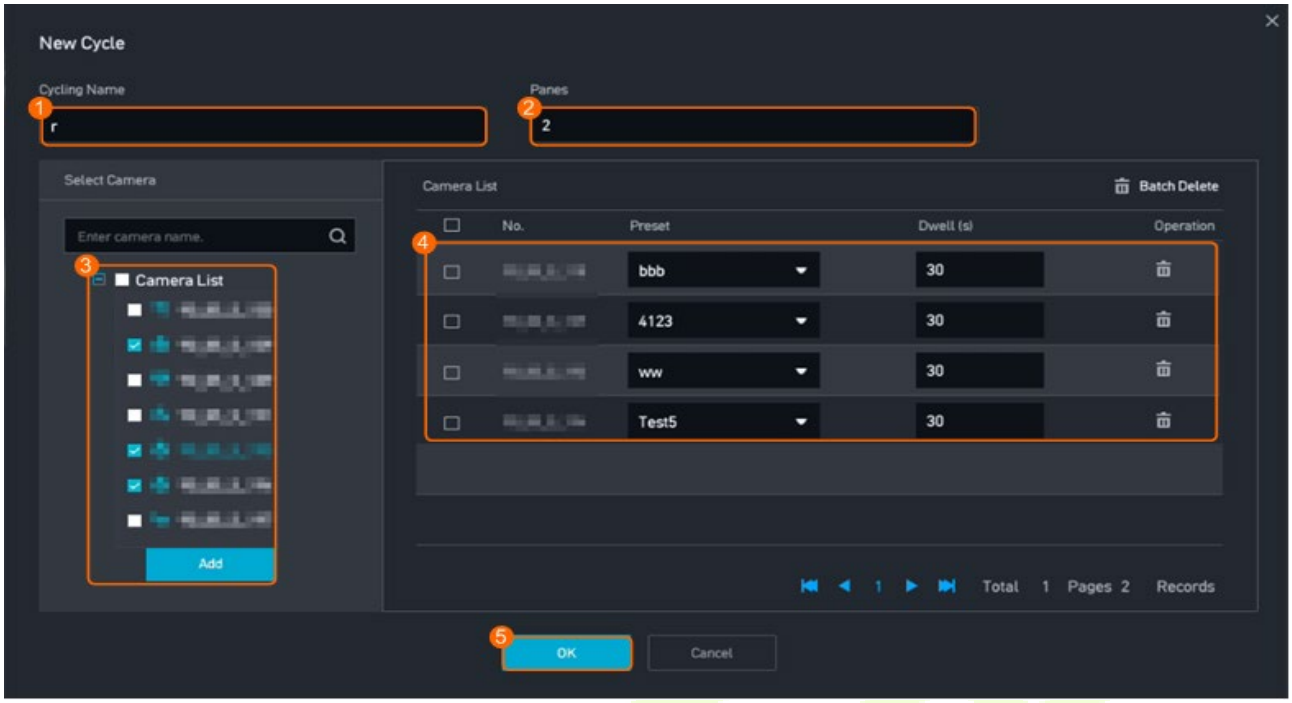
Procedure

Step 1 Log in to the LDU as the **admin** user.

Step 2 Click  in the lower left corner of the live video pane.

Step 3 Click  in the upper right corner of the list of cameras to cycle.

Step 4 Add a cycling policy, as shown in below.



Parameter Description

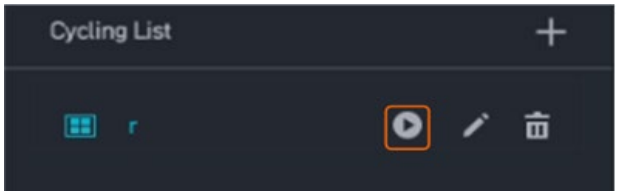
Parameter	Setting
Cycling Name	Set the name of a cycle group as required.
Camera List	Select cameras to be added to a cycle group in the device tree.
Panes	The number of cycling panes must be less than the number of cameras to cycle.
Preset	Select a preset position to view live video at the position during cycling.
Dwell (s)	Set the dwell duration for a camera to cycle as required.

Feature Verification

Step 1 Log in to the LDU as the **admin** user.

Step 2 Click in the lower left corner of the live video pane.

Step 3 Start camera cycling, as shown in below.



Step 4 Click next to any camera to stop the cycling.

4.1.3 Live Video View Management

Users can quickly invoke or restore preset live video views.

Application Scenario

- After a user adds live video from cameras at multiple intersections to favorites, the live video view is displayed upon each login.

Prerequisites

- You have commissioned real-time surveillance by referring to 4.1.1 Configuring Real-Time Surveillance.

Procedure

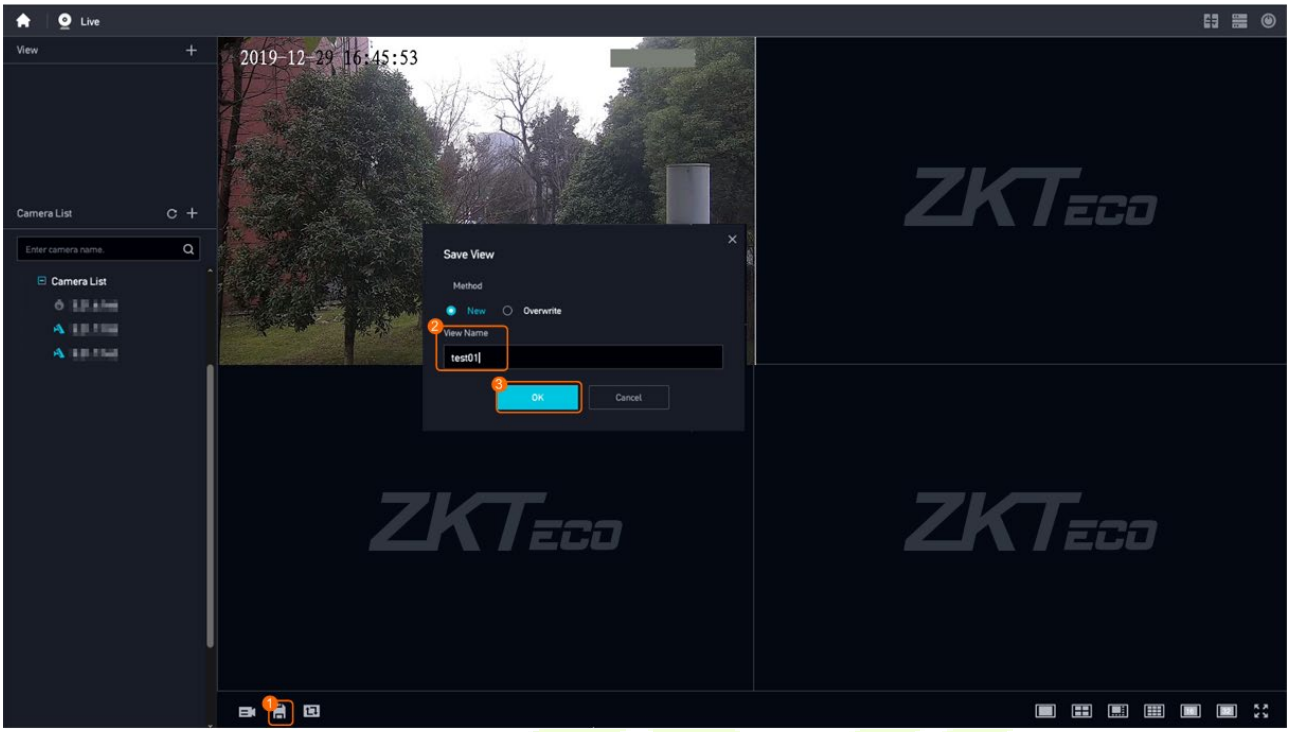
Step 1 Log in to the LDU as the **admin** user.

Step 2 Select a layout as required.

Step 3 The system supports the following layouts:  . In this example, select  .

Step 4 Select and drag cameras from **Camera List** to live video panes, as shown in below.

Step 5 Favorite the layout as a view, as shown in below.



- You can click  to create or overwrite a camera view in the layout.
- Then the view is displayed in the View area in the upper left corner of live video viewing page.

4.1.4 Voice Intercom

Definition

- Users can perform voice intercom with onsite personnel through cameras that are playing live video.

Customer Benefits

- Users can communicate with onsite personnel in a timely manner, improving communication efficiency.
- Onsite personnel can contact the surveillance center without using other devices, reducing user investment.

Application Scenario

- When an incident occurs, a user can use cameras to communicate with onsite personnel in real time.

Application Limitations

- A client supports only one channel of voice intercom.
- G.711U and G.711A are supported.

Prerequisites

- A camera supports the voice intercom function.
- A microphone and a speaker are available for the camera.
- A microphone and a speaker have been configured on the LDU.

Procedure

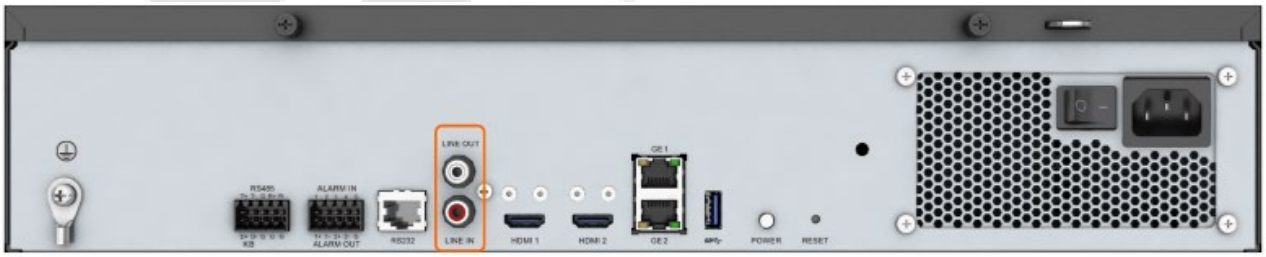
Step 1 Connect the microphone and speaker to the camera and the device.

1. Connect the microphone to the IN port of the camera, and connect the speaker to the OUT port of the camera.

   The ports vary depending on the camera model.

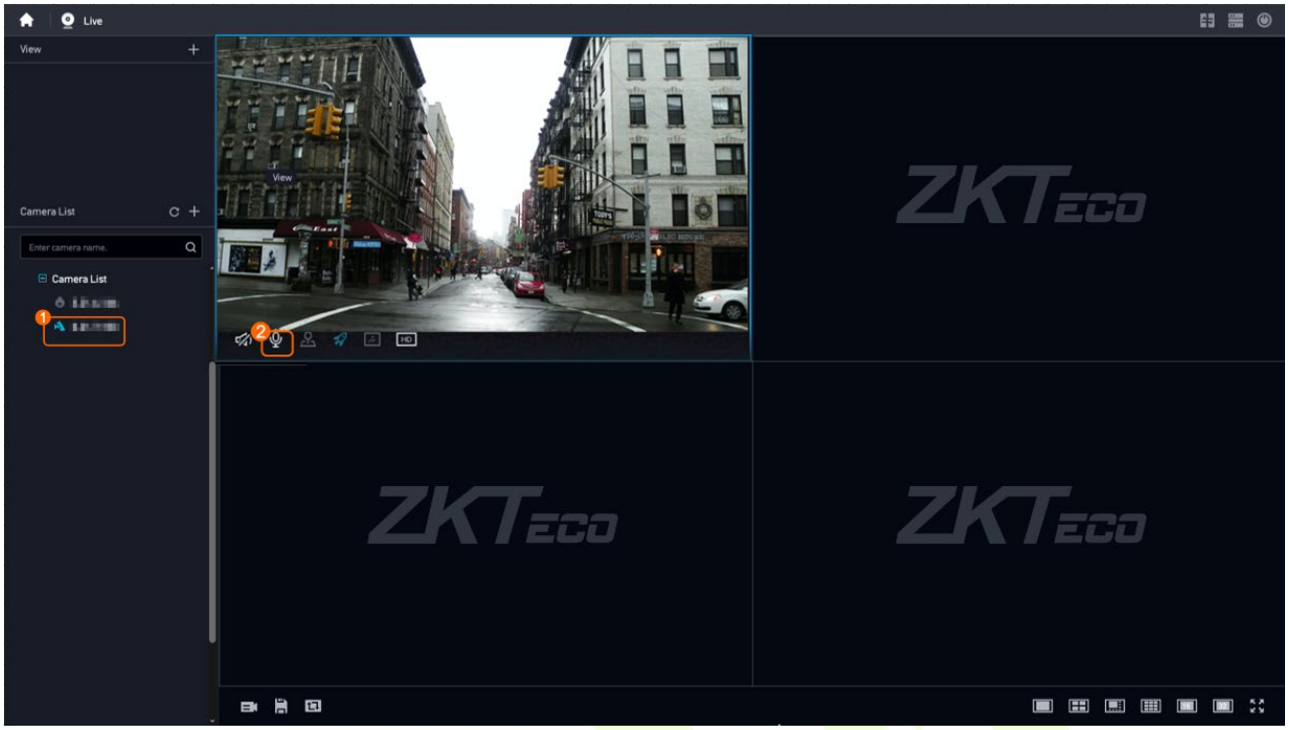
2. Connect the microphone to the LINE IN port on the rear panel of the device, and connect the speaker to the LINE OUT of the device, as shown in below.

   - **LINE OUT:** audio output port, which is used to receive audio from cameras.
   - **LINE IN:** audio input port, which can be used for voice broadcast or voice intercom with cameras with microphones.



Step 2 Enable the voice intercom function of the device.

1. Log in to the LDU as the admin user.
2. Drag a camera from the camera list to a live video pane.
3. Enable voice intercom, as shown in below.



Step 3 Talk with personnel at a surveillance site.

4.1.5 Channel-Associated Voice

Definition

- When users view live video or play back recordings, they can hear the voice in the video or recordings.

Application Limitations

- This feature is mainly applicable to indoor surveillance scenarios.
- To use this features, users need to configure a microphone for the camera.

Scenario Description

- Audio in live video

  For details about how to configure live video viewing, see 4.1.1 Configuring Real-Time Surveillance.
- Audio in recordings

  For details about how to configure video recording, see 4.2.1Configuring the Recording Parameters.

Prerequisites

- The camera has a sound pickup and is running properly.

- The audio device is running properly.

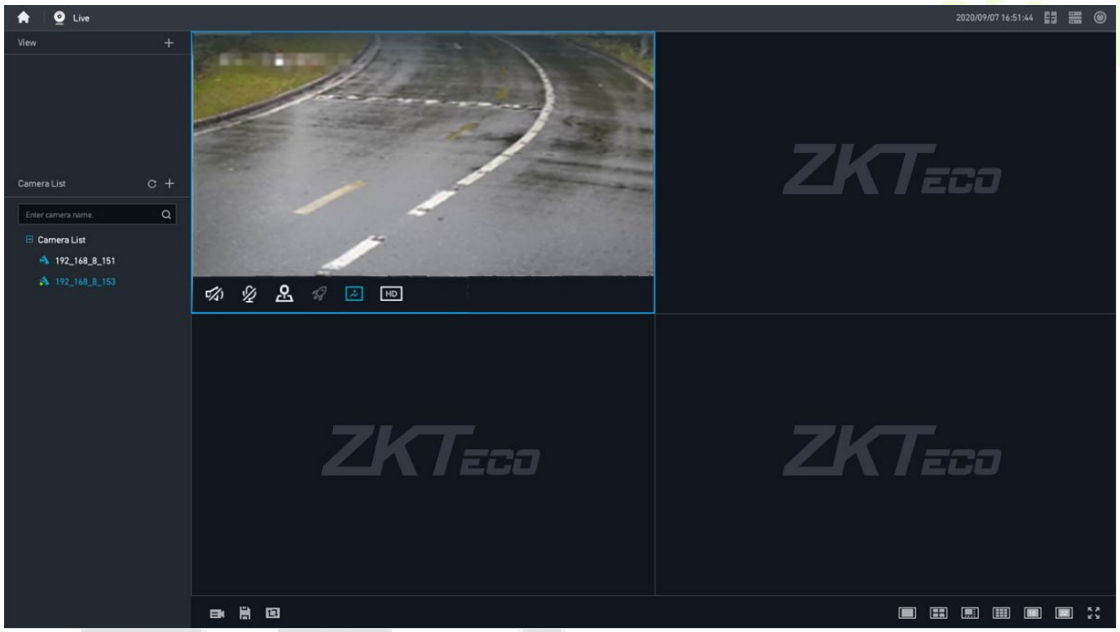
Procedure

- The procedure for enabling channel-associated voice in a live video pane is similar to that in a recording playback pane. The following describes how to enable channel-associated voice in a live video pane.

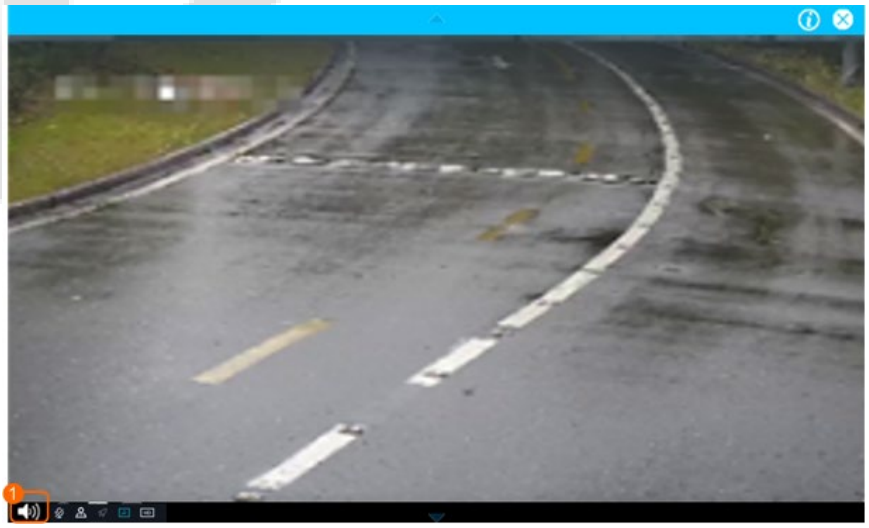
Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click the desktop and choose **Live** from the shortcut menu.

Step 3 In the camera list, double-click or drag an online camera to a live video pane, as shown in below.



Step 4 Enable channel-associated voice, as shown in below. Surveillance personnel can hear the voice at the surveillance site.



4.2 Playback

Users can view recordings to analyze incidents or abnormal situations that have occurred in surveillance areas.

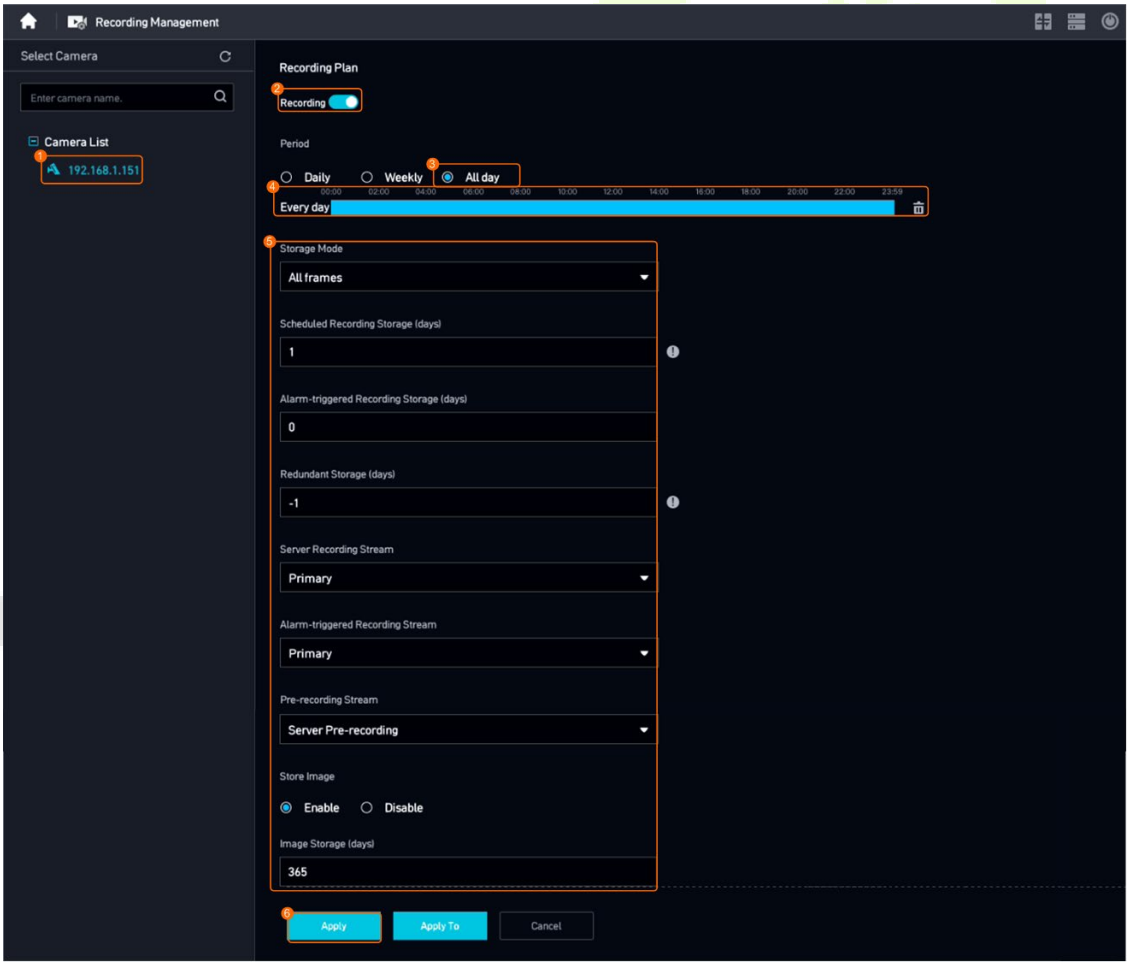
4.2.1 Configuring the Recording Parameters

- For personal privacy reasons, the recording function is disabled by default. To use the recording function, enable the recording function and set a recording plan by referring to this section. For specific settings, please refer to 4.7 Recording Management.

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **Recording Management**.

Step 3 Set recording management parameters and recording plans, as shown in below.



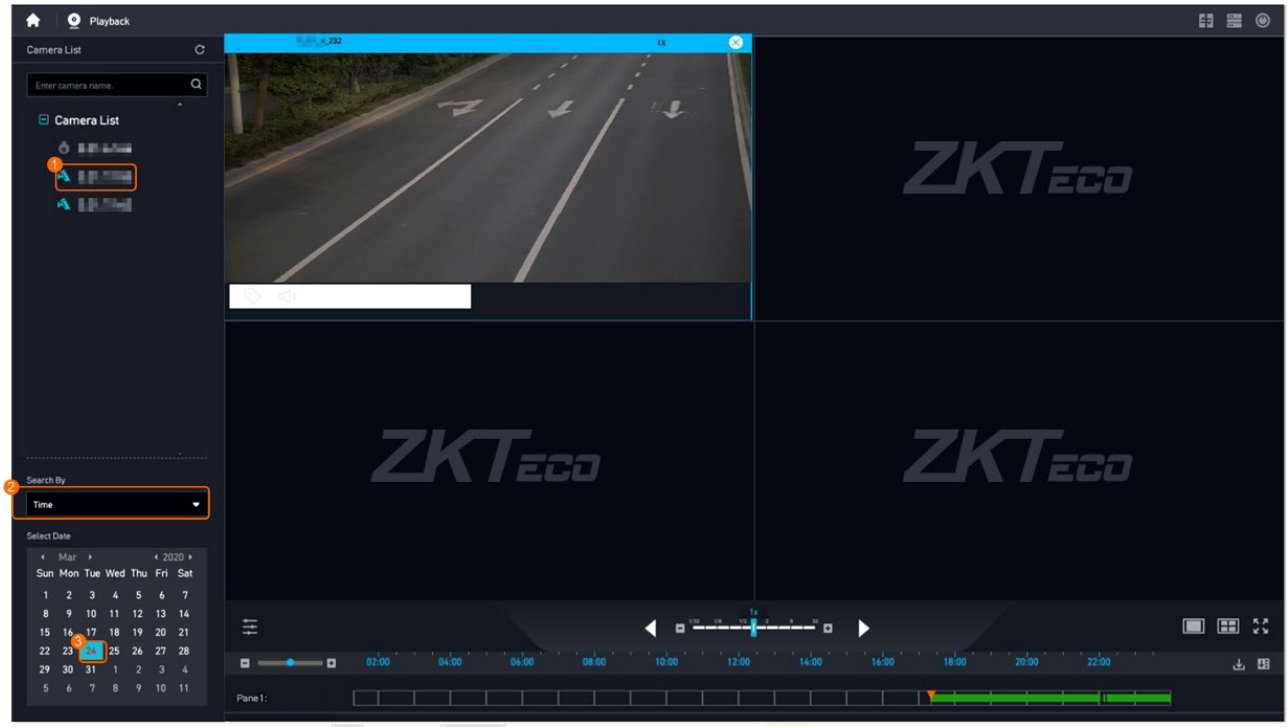
4.2.2 Playback Recording

- After the recording plan is enabled, wait for 10 minutes to generate camera recording files.

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **Playback**.

Step 3 Select the camera in the camera list, select the search method, and then select the date. Please note that the dates which there are video recordeds are displayed in green, as shown in the figure below.



Search By: Select a search mode as required. There are two query methods available by time and by bookmark.

Select Date: Click the date for search. The date, on which there is video recorded, is displayed in green.

Function Description

Icon	Function
	Adds bookmarks for recording files. Then you can search for recordings by bookmark.
	Enables the channel-associated voice function. Then you can hear voice from surveillance sites in real time through audio output devices.
	Simultaneously plays back recordings of multiple cameras from the same time point. For details, see 4.2.3 Simultaneous Playback of Multiple Recordings.
	Adjusts the recording playback speed and direction.

Icon	Function
	Selects a recording playback layout.
	Downloads recordings. For details, see 4.2.4 Recording Download.
	Views the recording download status.

4.2.3 Simultaneous Playback of Multiple Recordings

Definition

- Users can drag recordings from multiple cameras to multiple video panes on the screen and simultaneously play back the recordings.

Application Scenario

- A user simultaneously plays back multiple recordings to view the association between the recordings.

Application Limitations

- A maximum of four recordings can be played back at the same time.
- The network bandwidth needs to support simultaneous playback of multiple recordings.
- Users can control the simultaneous playback, including pause, resume, and quick locating.
- When a channel of recording playback fails or has no recording, other recording playback channels are not affected.

Prerequisites

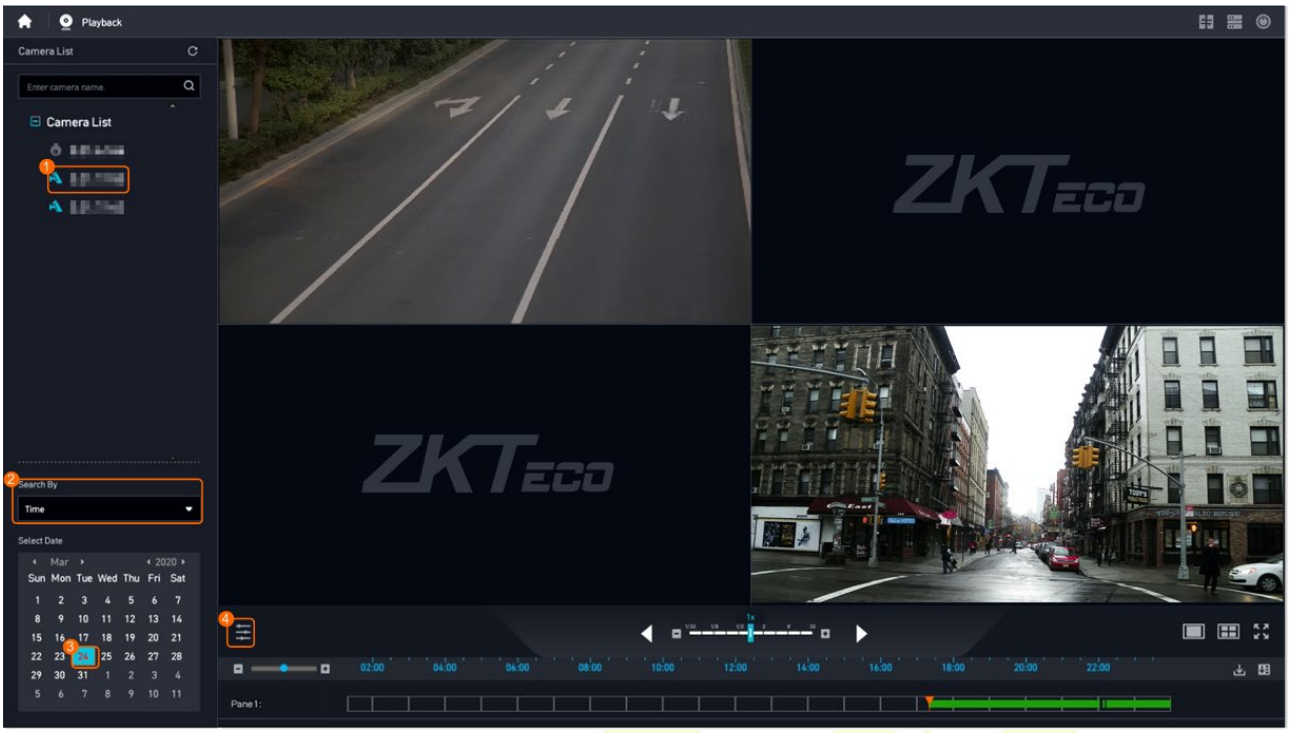
- For details about how to set recording parameters, see 4.2.1 Configuring the Recording Parameters

Procedure

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **Playback**.

Step 3 Play back recordings, as shown in below.



Parameter Description

Parameter	Setting
Query Mode	Query mode. There are two query methods, including By time and By bookmark.
Select Date	Click a date to query recordings. Dates with recordings are displayed in green.

4.2.4 Recording Download

Definition

- Users can download recording files to a local computer.

Application Limitations

- Downloaded recordings are saved in MP4 format.
- Server recordings can be downloaded at full speed (highest download speed provided by the system based on available resources).
- PU recordings cannot be downloaded.
- The downloaded recordings can be segmented by size that ranges from 200 MB to 3072 MB. The default size is 2048 MB.

- The downloaded recordings can be segmented by length that ranges from 5 minutes to 720 minutes. The default length is 30 minutes.
- Video files downloaded from the LDU cannot be played back using the Media Player or Thunder. You are advised to use the Storm Player, PotPlayer, or VLC.

Prerequisites

- A removable disk (such as a removable hard disk or USB flash drive) that uses the FAT32 or FAT file system is available.
- Check the file system of the removable disk as follows:
  1. Insert the removable disk into the USB port of the computer.
  2. Right-click the removable disk and choose **Properties** from the shortcut menu.
  3. Choose **General**.
  4. Check whether the file system is **FAT32** or **FAT**.

Procedure

Step 1 Insert the removable disk into the USB port of the backend device.

Step 2 Log in to the LDU as the **admin** user.

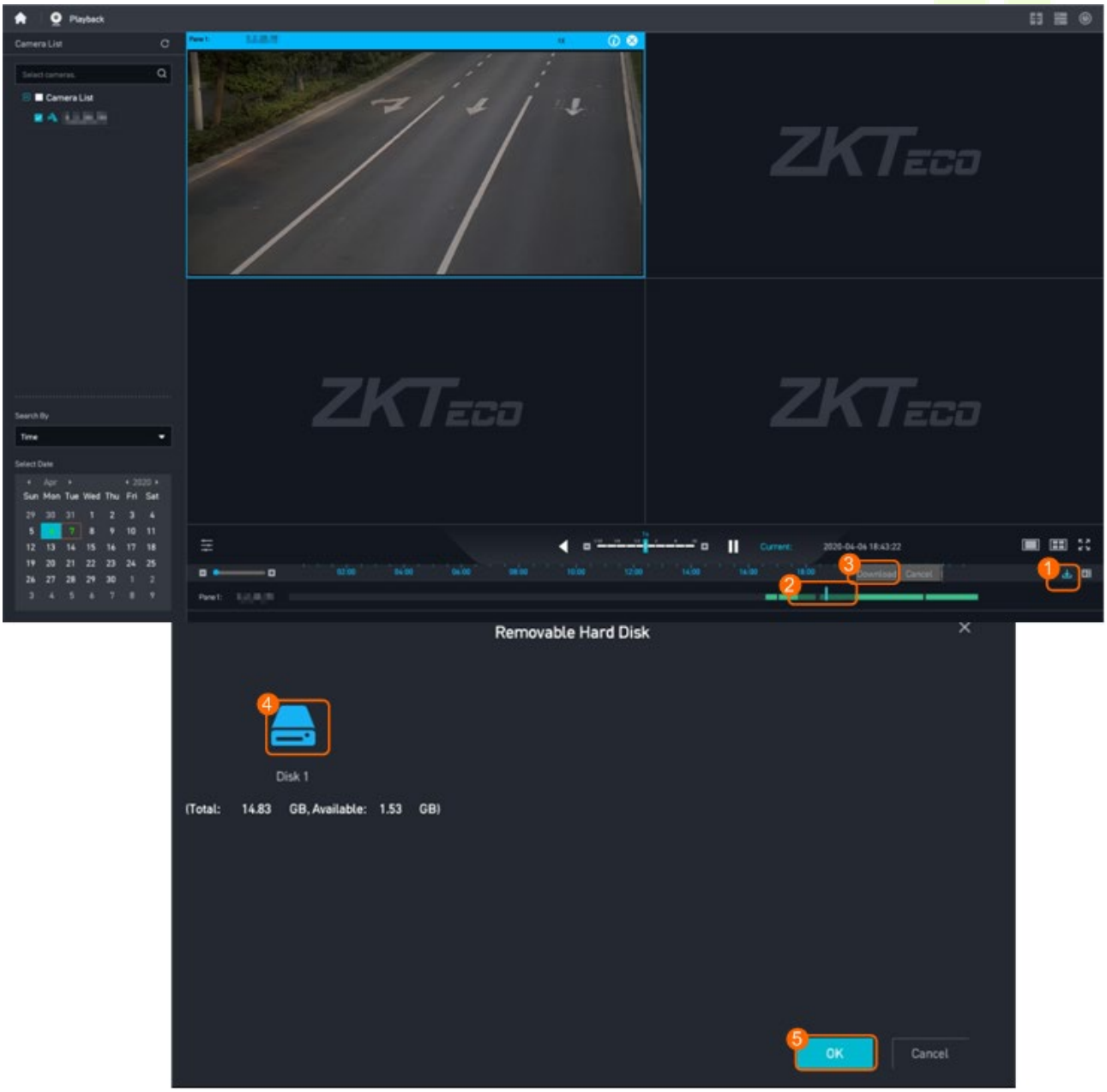
Step 3 Right-click on the desktop and choose **Playback**.

Step 4 Play back a recording, as shown in below.

Parameter Description

Parameter	Setting
Search By	Query mode. • Time • Bookmark
Select Date	Click a date to query recordings. Dates with recordings are displayed in green.

Step 5 Select recordings to download, as shown in below.



Step 6 Wait until the "Does the video need to be encrypted" is displayed.

1) If the recording file needs to be encrypted, select **Yes**.

   a. The encrypted recording file is stored in a .zip package on a removable disk.

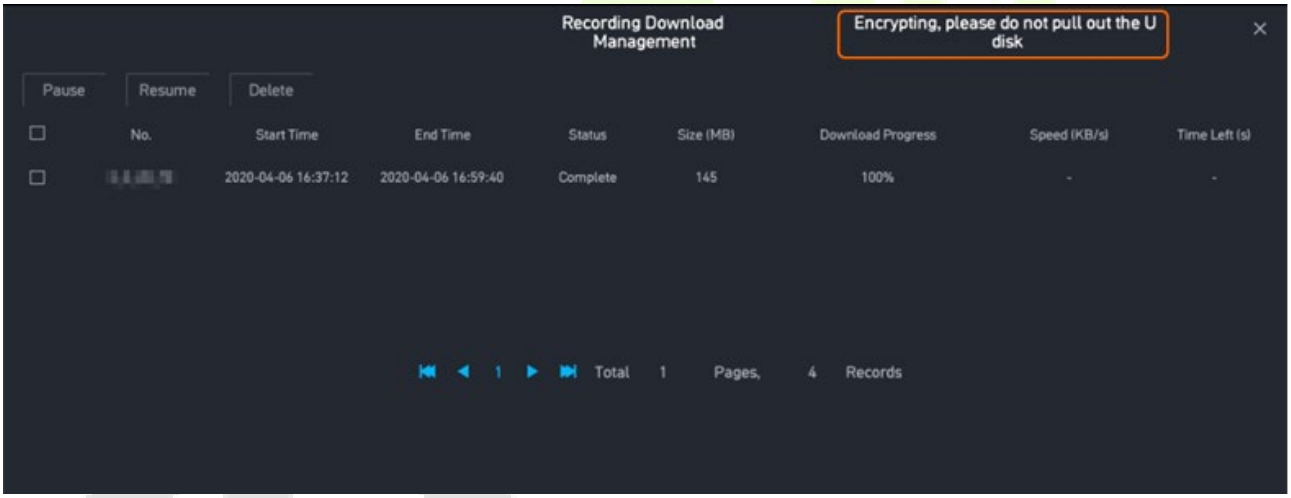
   b. Before downloading a recording file, you need to enter the password. The password is used to decompress the .zip package of the encrypted recording file on the computer.

      The password must meet the following requirements:

      - The password consists of 1 to 32 characters.
      - The password contains digits, uppercase letters, lowercase letters, and the following special characters: ! @ # $ % ^ & * ( ) + ~

   c. When the recording download progress reaches 100%, the system displays the "Encrypting, please do not pull out the U disk" message, as shown in below.

      In this case, the device is encrypting the recording files. Do not remove the USB flash drive. Otherwise, recording files will be lost. After the message disappears, remove the USB flash drive. The encryption duration varies depending on the file size.



2) If the recording file does not need to be encrypted, select **No**.

   For security purposes, you are advised to encrypt recording files.

   - Non-encrypted recording files are stored in MP4 format on removable disks and can be opened using a player on the computer.

4.3 Intelligent Applications

Prerequisites

- The facial recognition and face search algorithm plug-in packages have been installed.

- The facial recognition algorithm plug-in package varies depending on the device model. Install the plug-in package based on the site requirements. To check the device model, view the electronic label attached to the chassis or choose **Local Configuration** > **Basic Configuration** after logging in to the AS1700.

4.3.1 Search

- After the facial recognition service is configured in the system, AS1700 supports the retrieval of target persons in the results of face recognition intelligent analysis through "**Search by Image**" and "**Search by Criteria**".

Face Search by Image

After a face image is imported to the AS1700, the system automatically extracts facial features from the image and searches for the face based on the features.

Step 1 Check the file system of the removable disk and ensure that the removable disk uses the FAT32 or FAT file system.

a. Insert the removable disk into the USB port of the computer.

b. Right-click the removable disk and choose **Properties** from the shortcut menu.

c. Choose **General**.

d. Check whether the file system is **FAT32** or **FAT**.

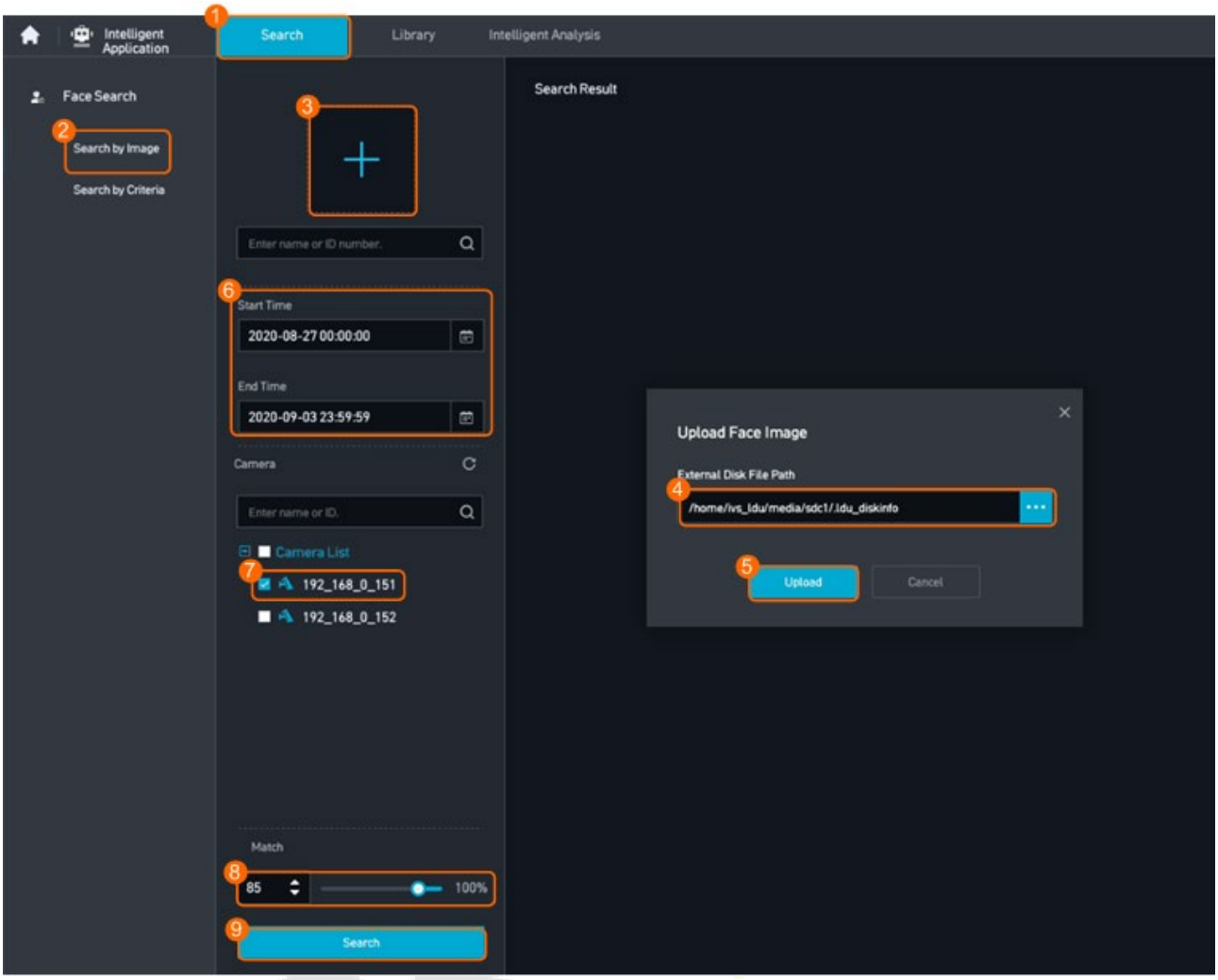
Step 2 Insert the removable disk into the USB port.

Step 3 Log in to the LDU as the **admin** user.

Step 4 Right-click on the desktop and choose **Intelligent Applications**.

Step 5 Choose **Search by Image** to configure face search.

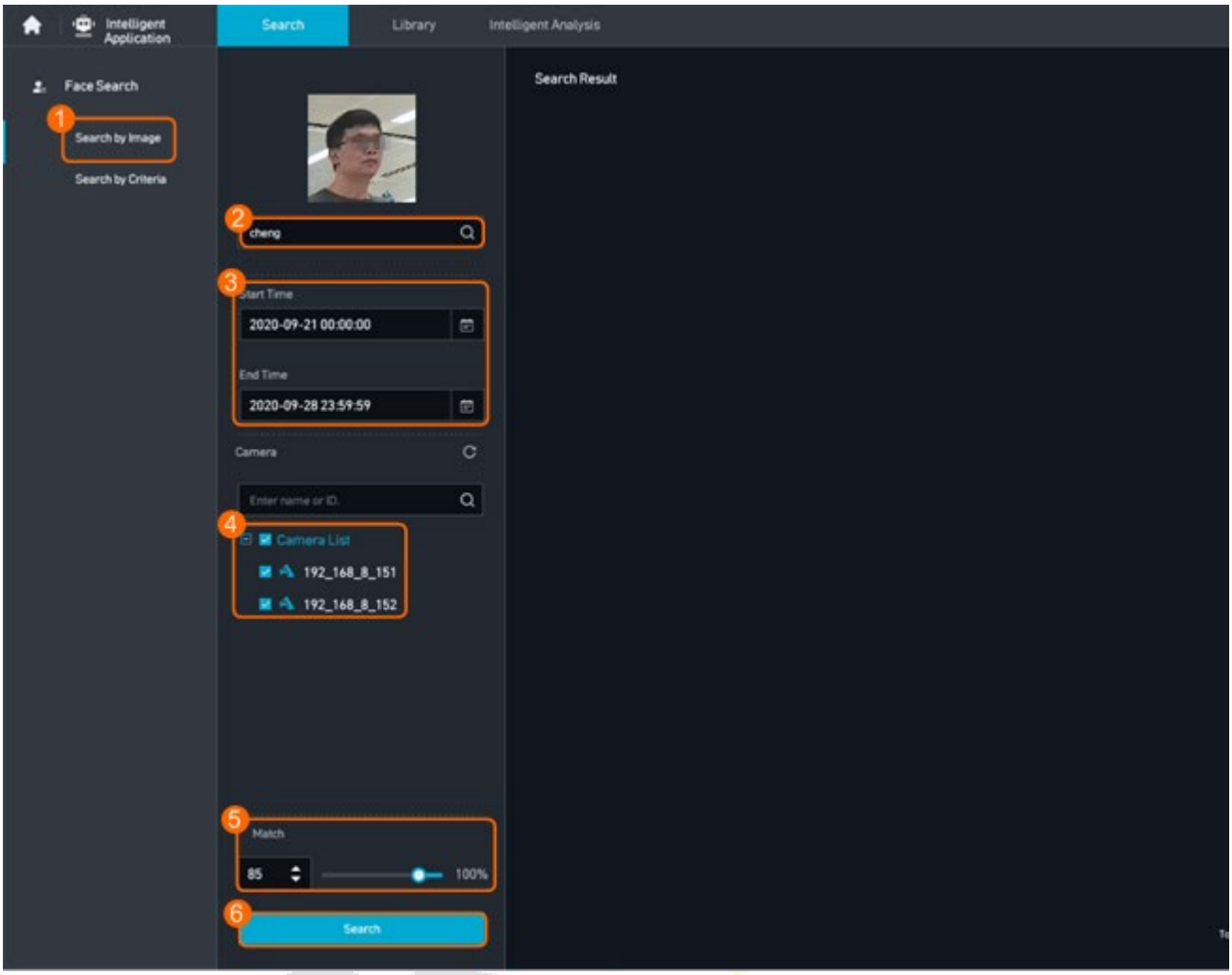
a. You can upload a face image from a removable disk, as shown in below.



Parameter Description

Parameter	Setting
Upload Face Image	Select a face image stored in the removable disk. The characters in face image names must be encoded in GBK or UTF-8 format. If the encoding format is not GBK or UTF-8, correct it. Face image names encoded in other formats will be displayed in garbled characters on the LDU.
Start Time/End Time	Set the search period as required.
Device	Select cameras from the camera list based on the site requirements.
Match	Customize the similarity. Face images whose similarity is greater than or equal to the specified value can be displayed.

b. Enter the full name or ID in the search box, select a face image from the face library, and start image search, as shown in below.

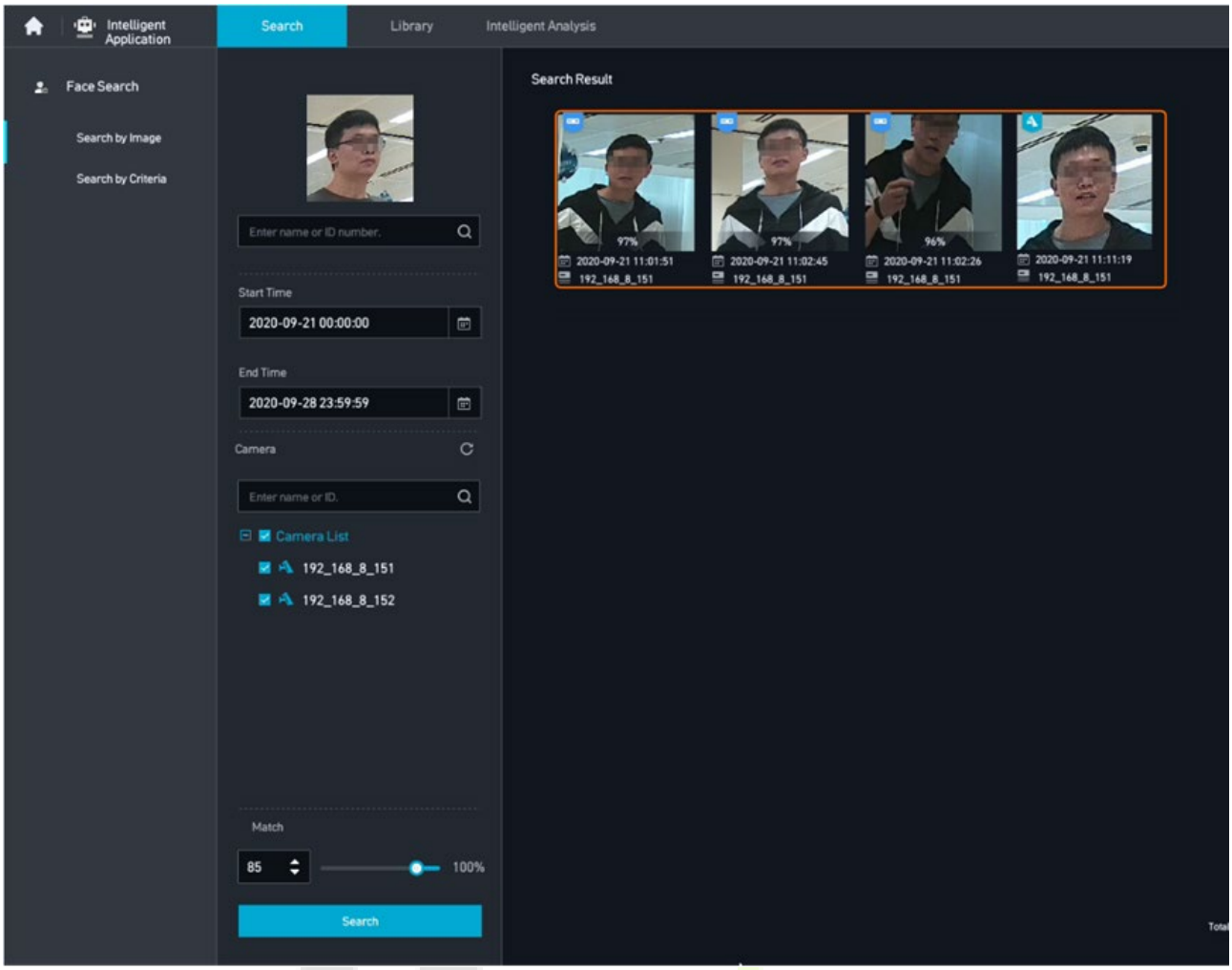


Step 6 View the search results.

The system searches for images similar to the uploaded images, as shown in below. In this example, an image is uploaded from a removable hard disk for face search.

 indicates the face image extracted by the intelligent facial recognition task in the AS1700.

 indicates the face image captured by the camera after facial recognition is enabled and subscribed by the AS1700.



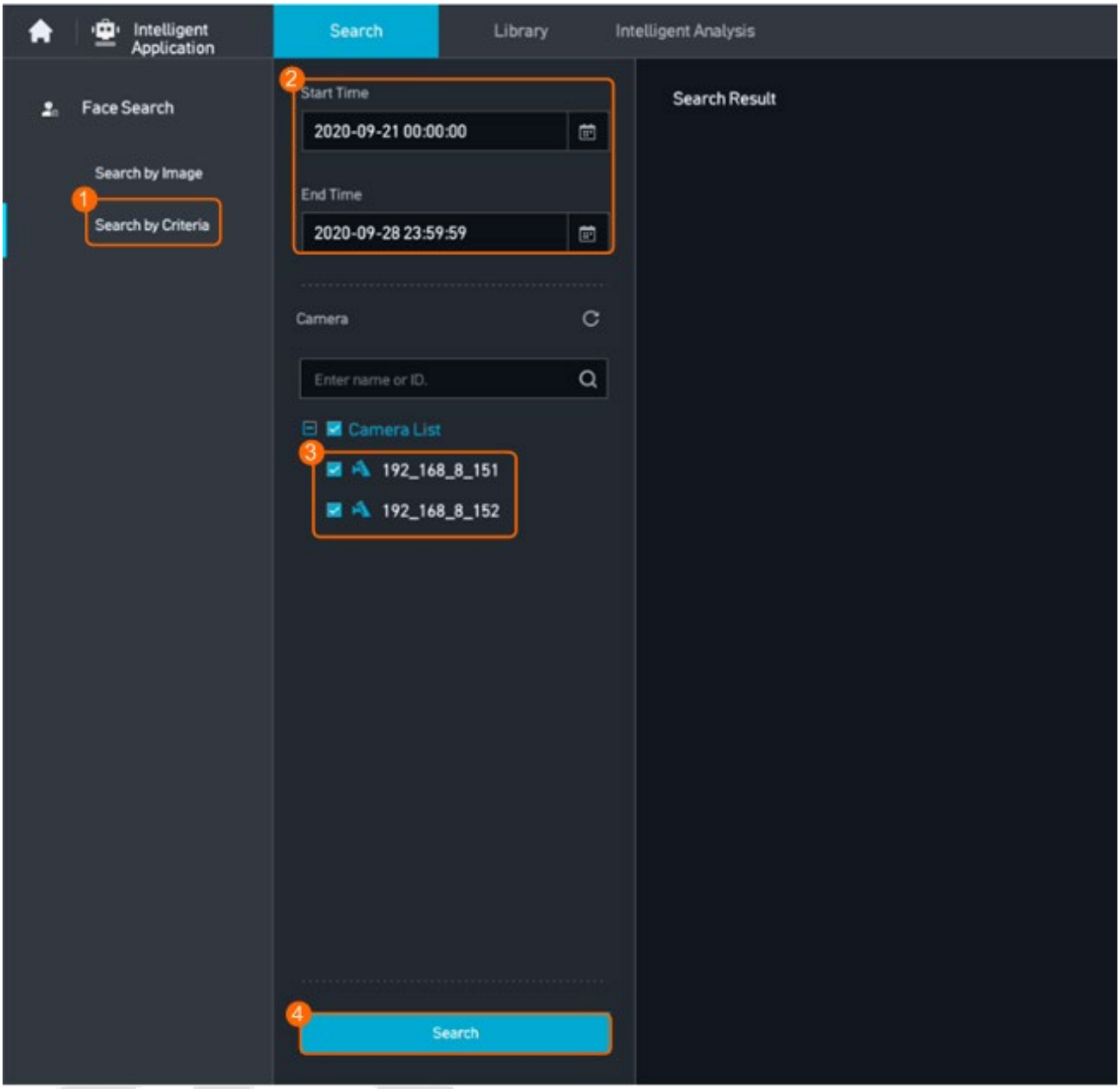
Face Search by Criteria

After face search criteria are entered, the system searches for face images based on the search criteria.

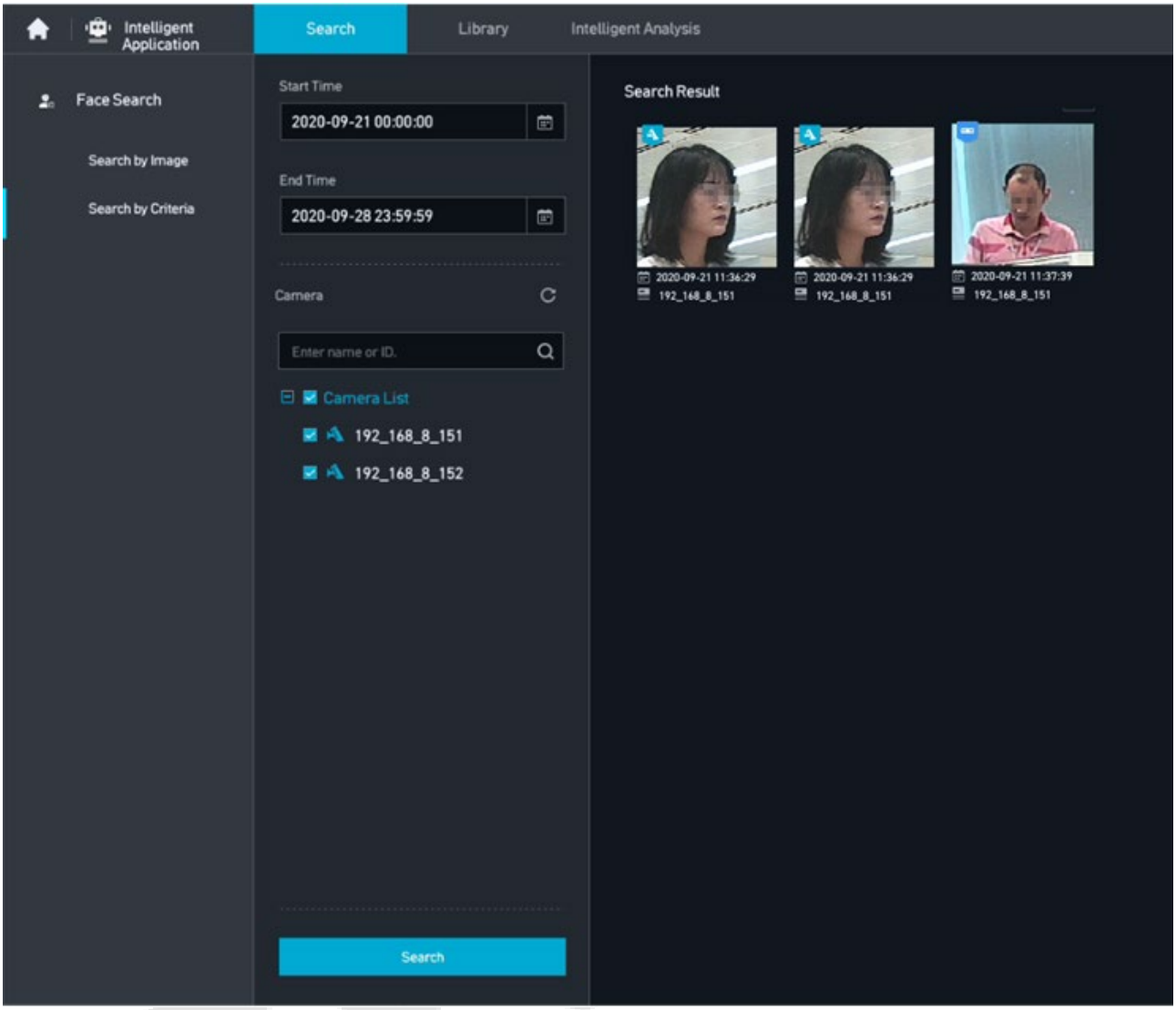
Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **Intelligent Applications**.

Step 3 Choose **Search by Criteria** to configure face search, as shown in below.



Step 4 View the search results, as shown below.

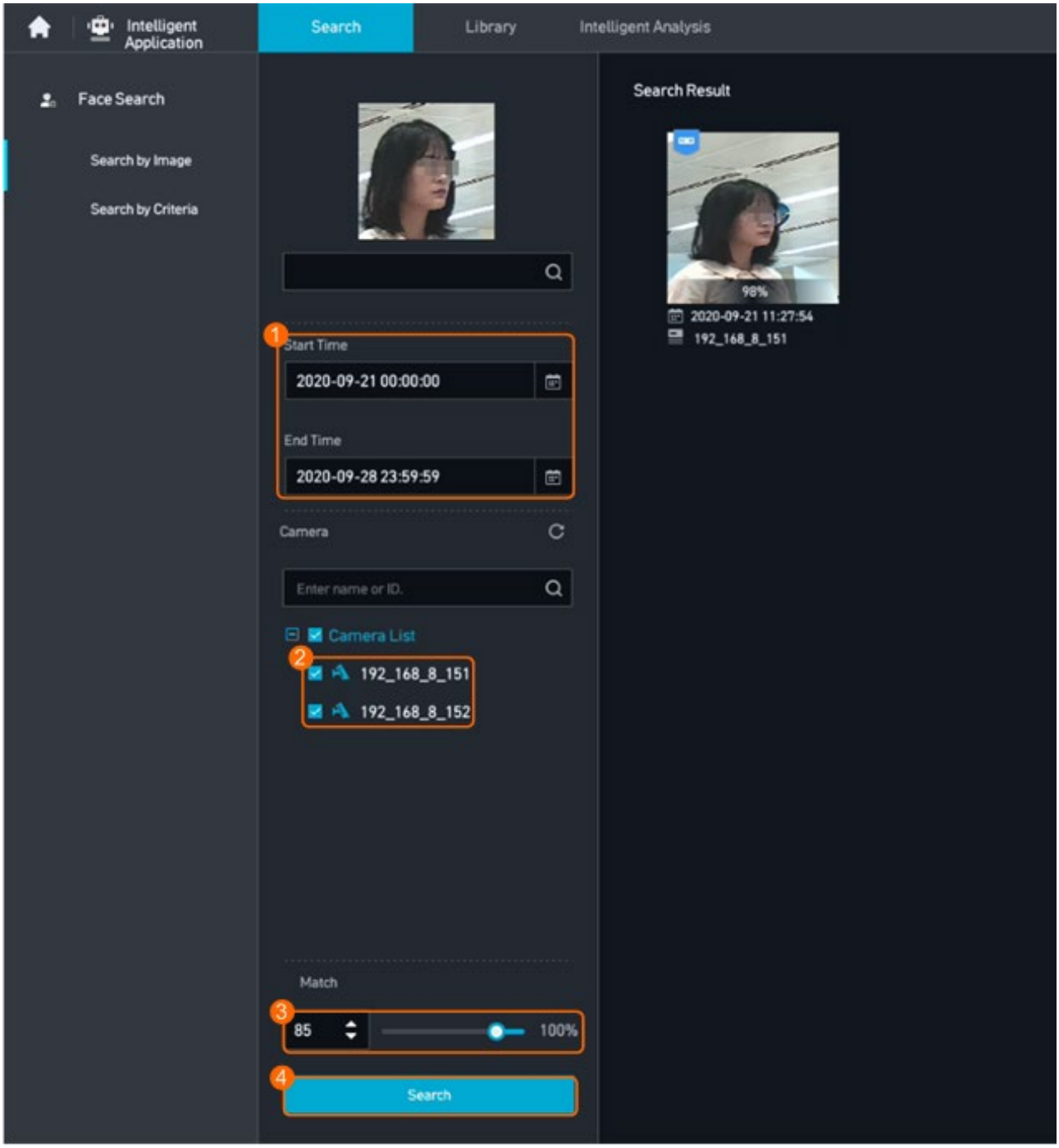


Step 5 (Optional) Use a clear target face image for secondary search to obtain more images of the target face.

a. Click a search result.

b. On the result details page, perform secondary search.

c. Configure secondary search criteria, as shown in below.



4.3.2 Library

Context

- The LDU supports only the face blacklist.

Prerequisites

- A removable disk (such as a removable hard disk or USB flash drive) that uses the FAT32 or FAT file system is available.

  Check the file system of the removable disk.

  1) Insert the removable disk into the USB port of the computer.
  2) Right-click the removable disk and choose **Properties** from the shortcut menu.
  3) Choose **General**.
  4) Check whether the file system is **FAT32** or **FAT**.

- Face images have been named as required and stored in a removable disk (such as a removable hard disk or USB flash drive).
  - Batch import: Select a folder to upload the images in it. The images are named in ***Name_ID number_ID type_Sex_Nationality_Occupation*** format.

    A maximum of 16,000 face images can be stored in a single folder on a removable disk (such as a removable hard disk or USB flash drive) of the **FAT32** or **FAT** file system. If more than 16,000 face images need to be imported, create multiple folders and import them in batches.
  - Upload one by one: The image is named after the name.

NOTE:

- Face images in the face library must meet the following requirements:
- Image format: Only .bmp, .dib, .jpe, .jpeg, .jpg, and .png images are supported.
- Image size: The recommended image size is 35 KB to 200 KB. The size of a single image cannot exceed 720 KB.
- Image quality: The face in the image must be clear. The image must be a grayscale image of eight bits or more.
- Resolution: The recommended face resolution ranges from 80 x 80 to 200 x 200 pixels. The eye spacing must be greater than or equal to 60 pixels, and eye spacing of 90 pixels or more is recommended.

- Brightness and contrast: The ambient illumination must be at least 300 lux. Use diffuse lighting for the best effect. The contrast should be moderate, and the face should not be shadowed. Avoid backlight and light reflection, and use a moderate exposure.
- Posture: Use proper posture and look straight ahead. The yaw angle, pitch angle, and roll angle of the face should be within the range of –10° to +10°.
- Blocking: The eyebrows, eyes, mouth, nose, and face contours must not be blocked by hair, mouth mask, accessories, or glasses. If glasses are worn, the lenses should be clear and non-reflective.
- Face: A complete, clear, unretouched image of the face is required. The contour and facial features should be clear, and heavy makeup should be avoided.
- Facial expression: The person should wear a neutral expression, with eyes open and mouth closed naturally. Laugh, frown, or other strong expressions should be avoided.
- Encoding requirement: The characters in face image names must be encoded in GBK or UTF-8 format. If the encoding format is not GBK or UTF-8, correct it. Face image names encoded in other formats will be displayed in garbled characters on the LDU.

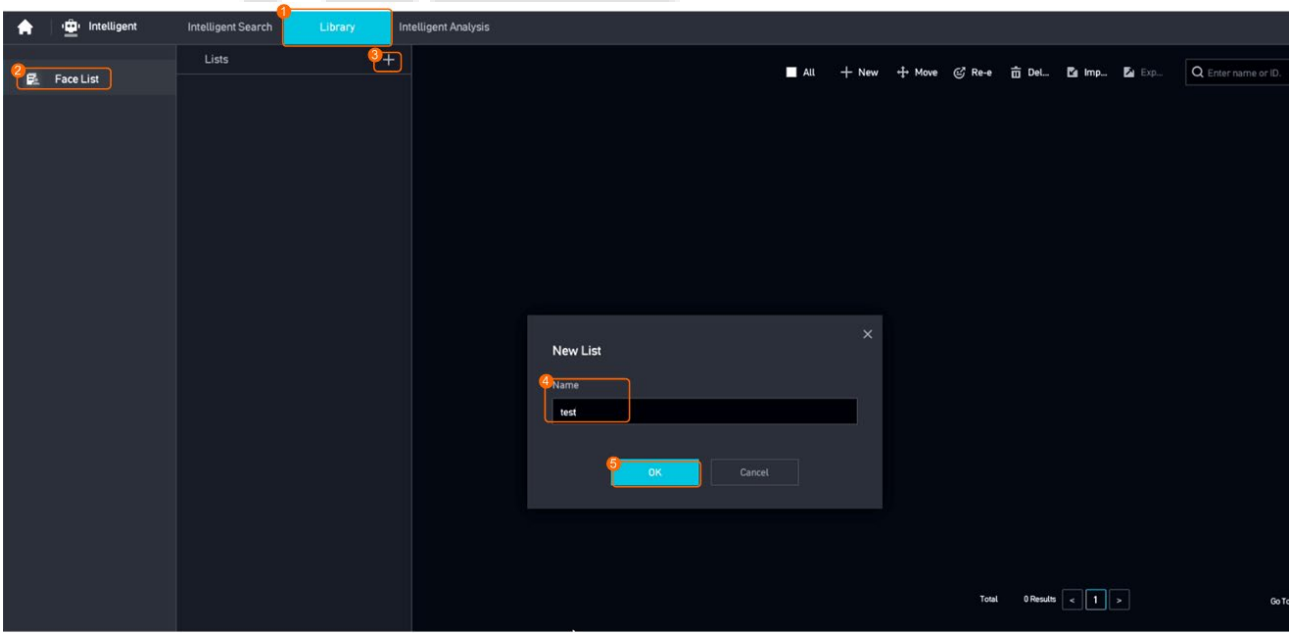
Procedure

Step 1 Insert the removable disk into the USB port.

Step 2 Log in to the LDU as the **admin** user.

Step 3 Right-click on the desktop and choose **Intelligent Applications**.

Step 4 Configure a face list, as shown in below.

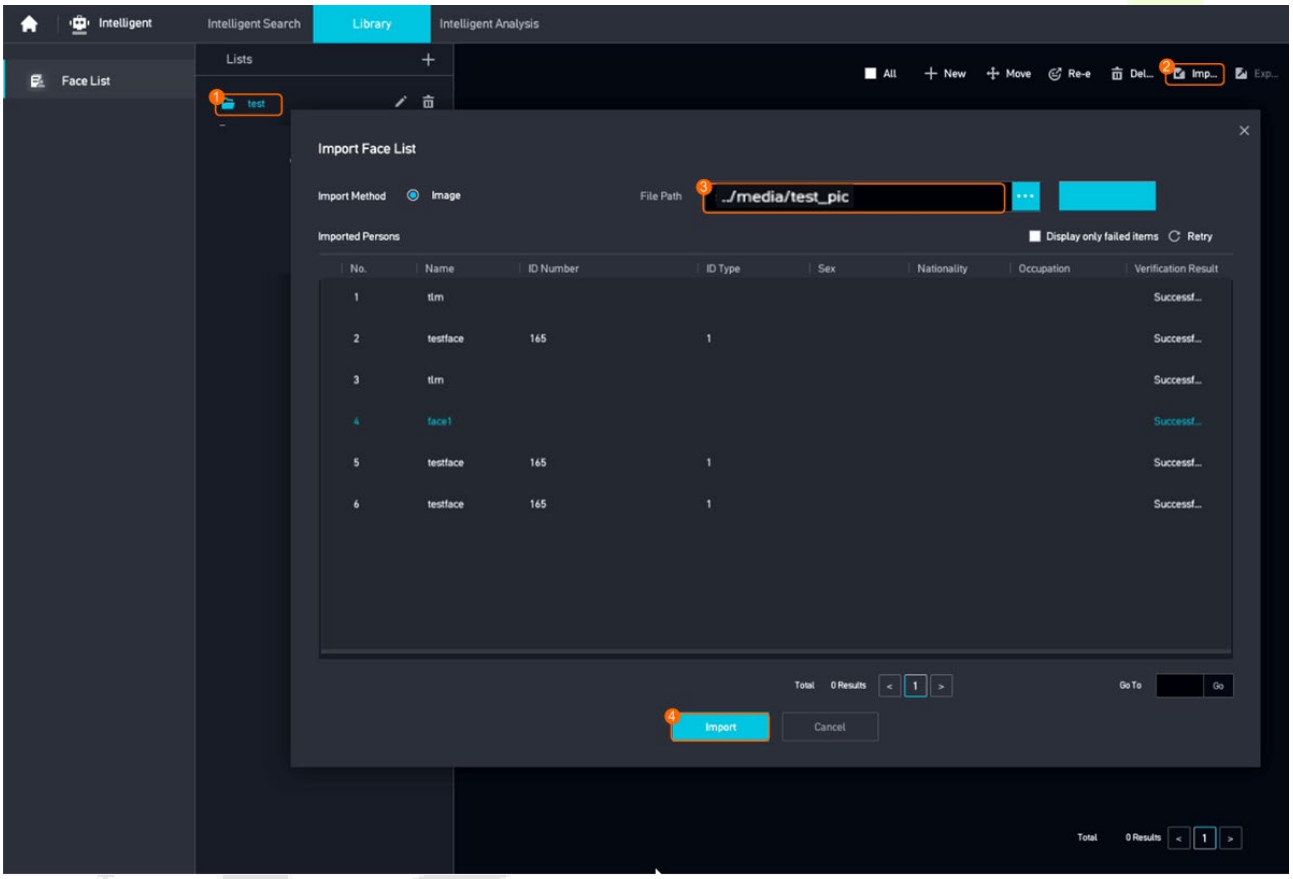


Parameter Description

Parameter	Setting
Name	Customize a face list name. You can edit and modify the created face lists. The system supports a maximum of 32 face lists.

Step 5 Add face information.

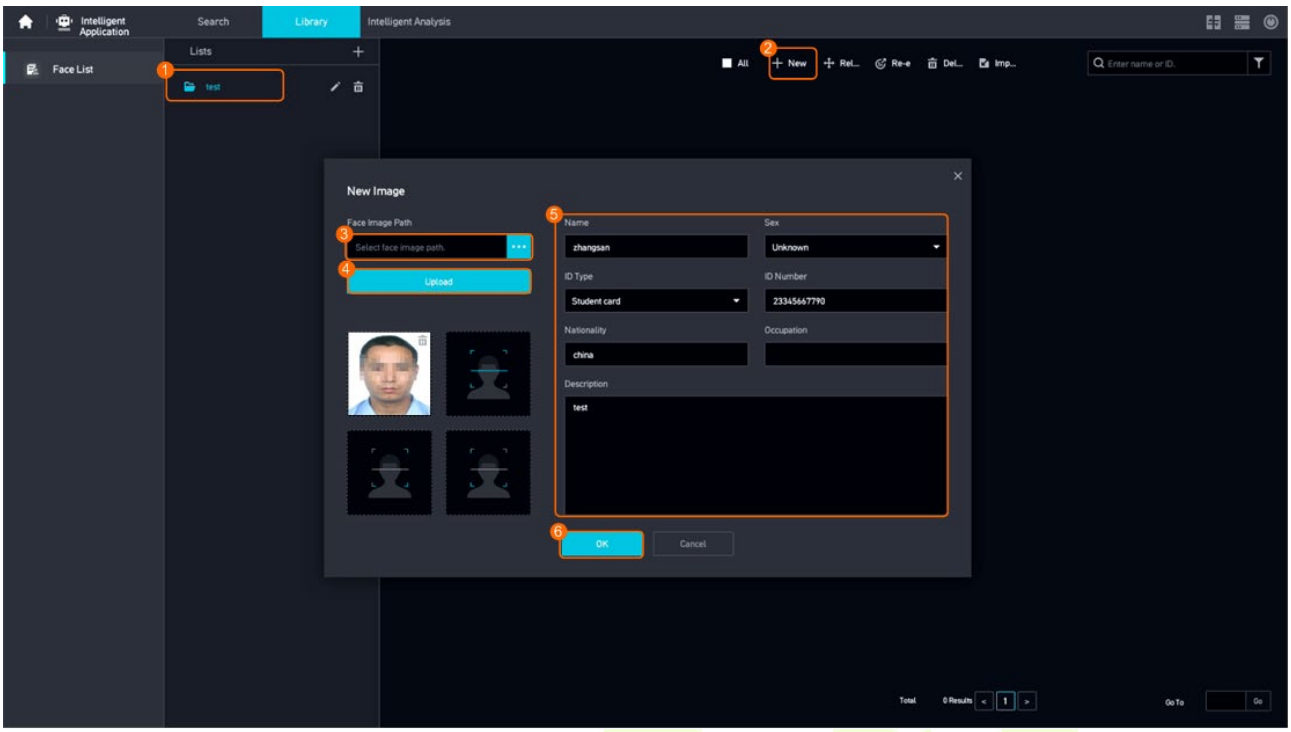
- Import face images, as shown in below.



Parameter Description

Parameter	Setting
File Path	Select the folder where face images are located.

- Add faces one by one, as shown in below.



Parameter Description

Parameter	Setting
Face Image Path	Select a face image stored in the hard disk.
Name	Set these parameters based on the site requirements.
Sex	
ID Type	Set these parameters based on the site requirements.
ID Number	
Nationality	Set these parameters based on the site requirements.
Occupation	
Description	Customize the face description as required to identify the face.

4.3.3 Intelligent Analysis

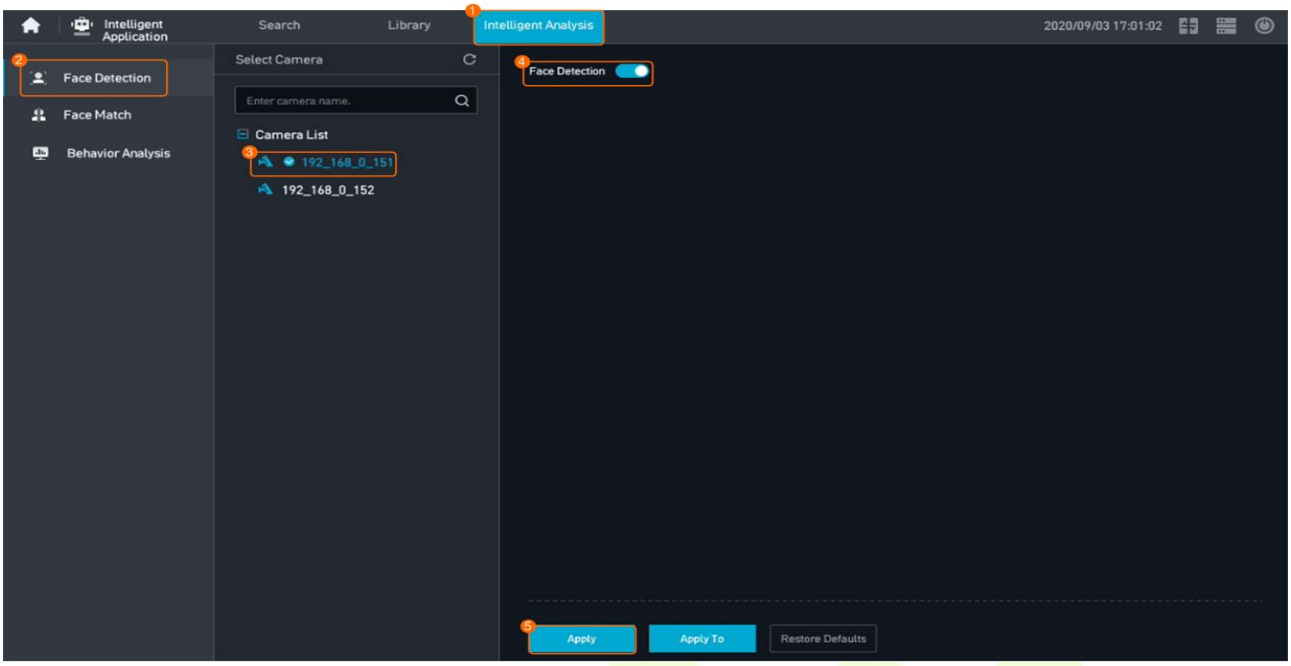
4.3.3.1 Face Detection

Users can configure face recognition tasks here.

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **Intelligent Applications**.

Step 3 Choose **Face Detection** to configure facial recognition, as shown in below.



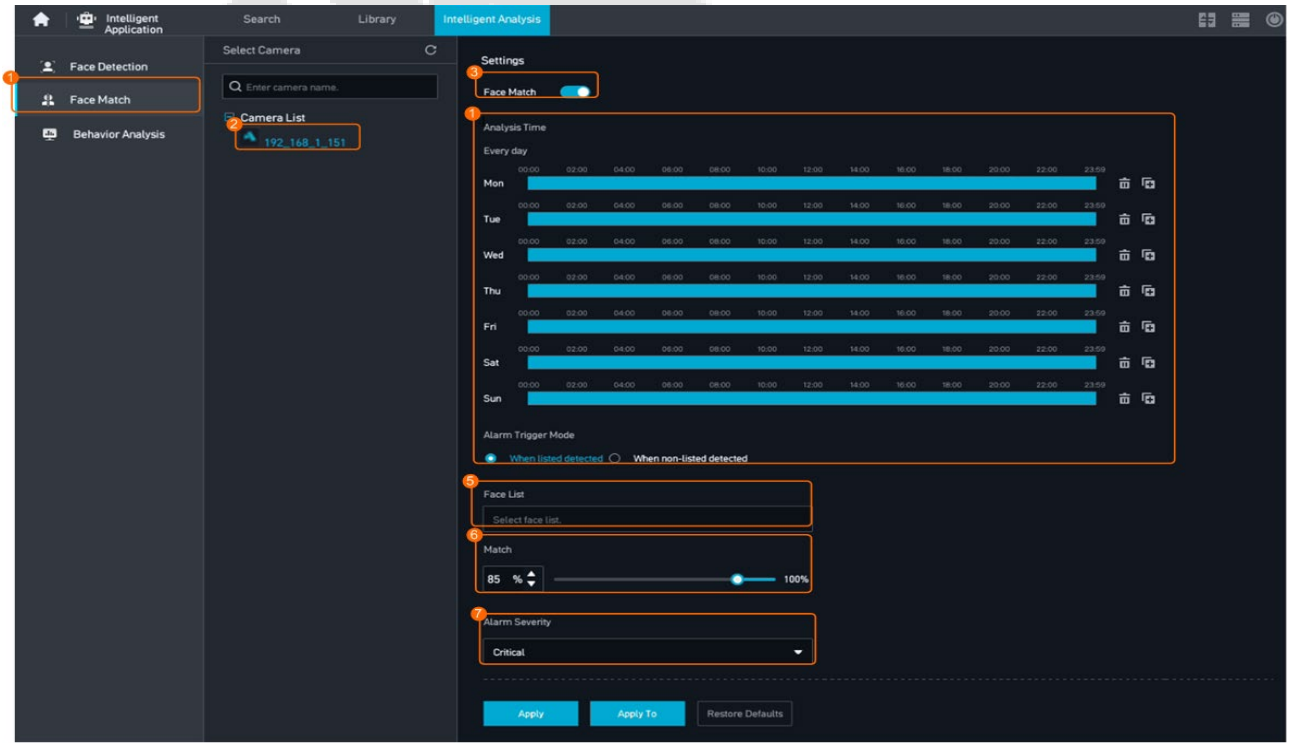
4.3.3.2 Face Match

Users can configure a face alert here.

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **Intelligent Applications**.

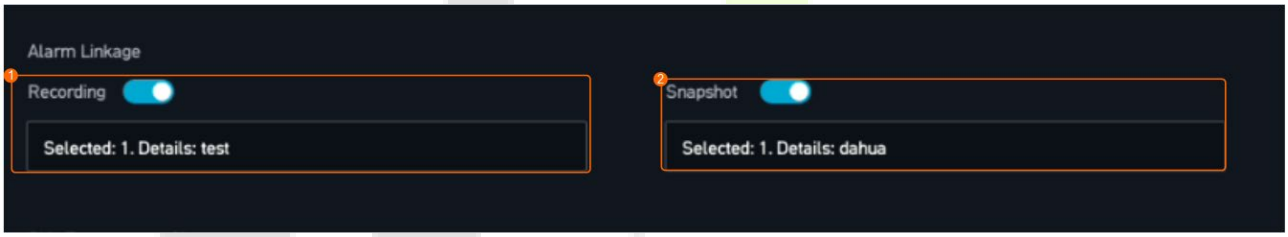
Step 3 Configure a face alert, as shown in below.



Parameter Description

Parameter	Setting
Face Match	Enable **Face Match**.
Analysis Time	Set the daily analysis period based on the site requirements.
Alarm Trigger Mode	Set this parameter based on the site requirements. • **When listed detected:** When the recognized face matches the target face of the face alert task, an alarm is generated. • **When non-listed detected:** When the recognized face does not match the target face of the face alert task, an alarm is generated.
Face List	Select a face list based on the site requirements.
Alarm Severity	Set this parameter based on the site requirements.
Match	Customize the similarity. • When the similarity between a passer-by face and the target face is greater than or equal to the specified value, the two faces match. • When the similarity between a passer-by face and the target face is less than the specified value, the two faces do not match.

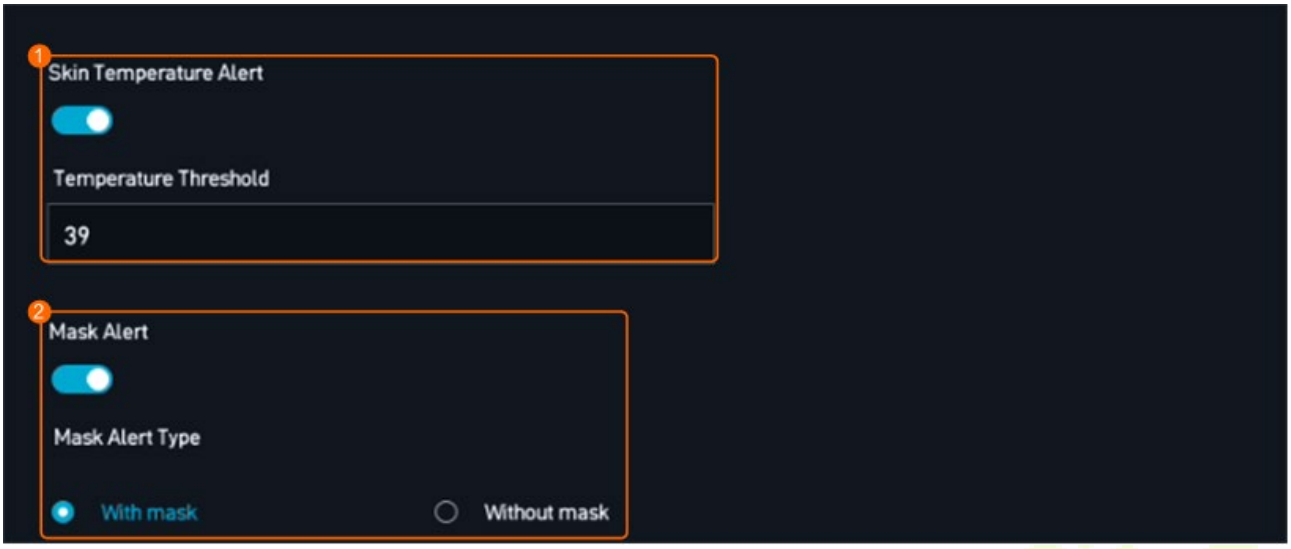
Step 4 (Optional) Configure alarm linkage, as shown in below.



Parameter Description

Parameter	Setting
Alarm Linkage Recording	Select a camera based on the site requirements. When the face alert task of the camera generates an alarm, the system triggers the selected camera to record video.
Snapshot	Select a camera based on the site requirements. When the face alert task of the camera generates an alarm, the system triggers the selected camera to take snapshots.

Step 5 (Optional) Configure the body temperature alarm and mask alarm, as shown in below.



Parameter Description

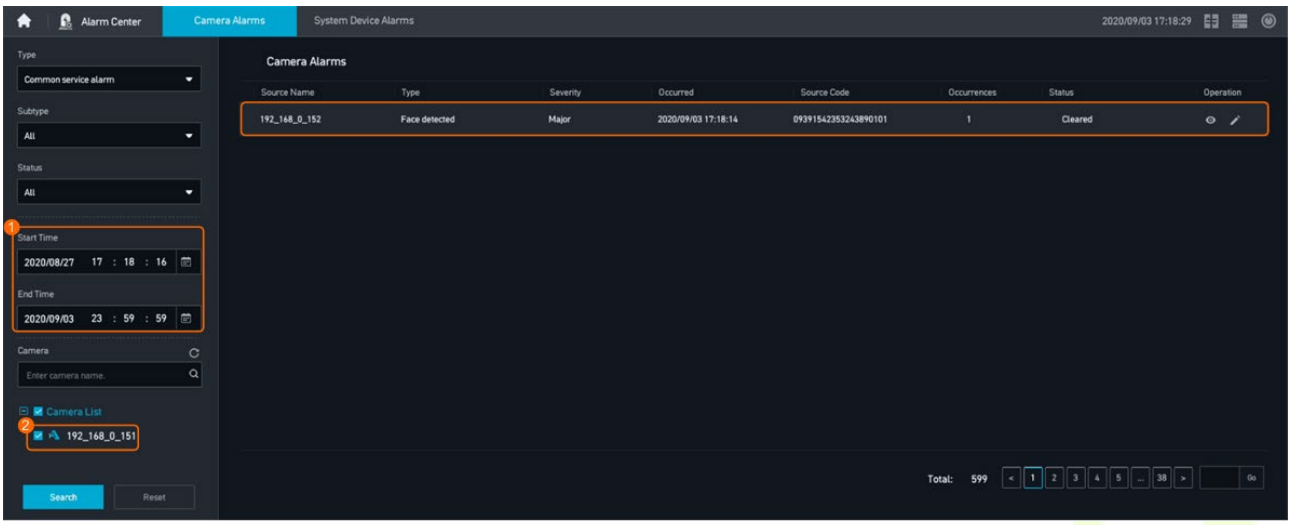
Parameter	Setting
Skin Temperature Alert	Enable **Skin Temperature Alert**. The temperature threshold range is 35.0℃~43.0℃. The user sets the skin temperature alert value according to actual needs. When the human body temperature is greater than the deployment control threshold, an alarm will be generated. **Note:** The current skin temperature alert only supports designated temperature measuring devices. Please contact technical support for how to access it.
Mask Alert	Indicates whether to enable the mask detection alarm function.
Mask Alert Type	Mask alert type. After **Mask Alert** is enabled, select an alert type as required. The options are as follows: • **Without mask**: An alarm is generated when the system detects a person wearing no mask. • **With mask**: An alarm is generated when the system detects a masked person.

Step 6 Search for alarms generated by the face alert task

1) Right-click the on desktop and choose **Alarm Center**.

2) Search for alarms generated by the face alert task, as shown in below.

A face alert alarm is generated only when a camera matches face information in the face list.



3) Click to view alarm details.

- Click **Triggered Snapshot** to view the snapshots taken when the alarm is generated.
- Click **Triggered Recording** to view the video recorded when the alarm is generated.

4) Click to acknowledge the alarm and add description.

4.3.3.3 Configuring Behavior Analysis

- You can configure multiple types of behavior analysis rules on the LDU. Different types of behavior analysis rules apply to different scenarios. Typical application scenarios are shown in the following table.

Typical application scenarios

Behavior Analysis Rule	Typical Application Scenario
Intrusion detection	Mainly applied to borders or fences of important areas to prevent dangerous events from happening because of invasion of outsiders.
Loitering detection	Mainly applied to areas like ATMs of a bank where people flow is low. It is used to detect suspicious people in advance.
Tripwire crossing detection	Mainly applied to caution belts used in borders of important areas. It generates an alarm when an object crosses the pre-defined tripwire and continue to move in the prohibited direction.
Fast movement detection	Mainly applied to campus roads and country roads with a low object flow. It is used to detect objects that move at a speed higher than the maximum speed.
Area entry detection	Mainly applied to a specified space in an important area. It generates an alarm when a person enters into this space.

Behavior Analysis Rule	Typical Application Scenario
Area exit detection	Mainly applied to monitor valuable assets in a specific space. It generates an alarm when objects leave this space.

Intrusion detection

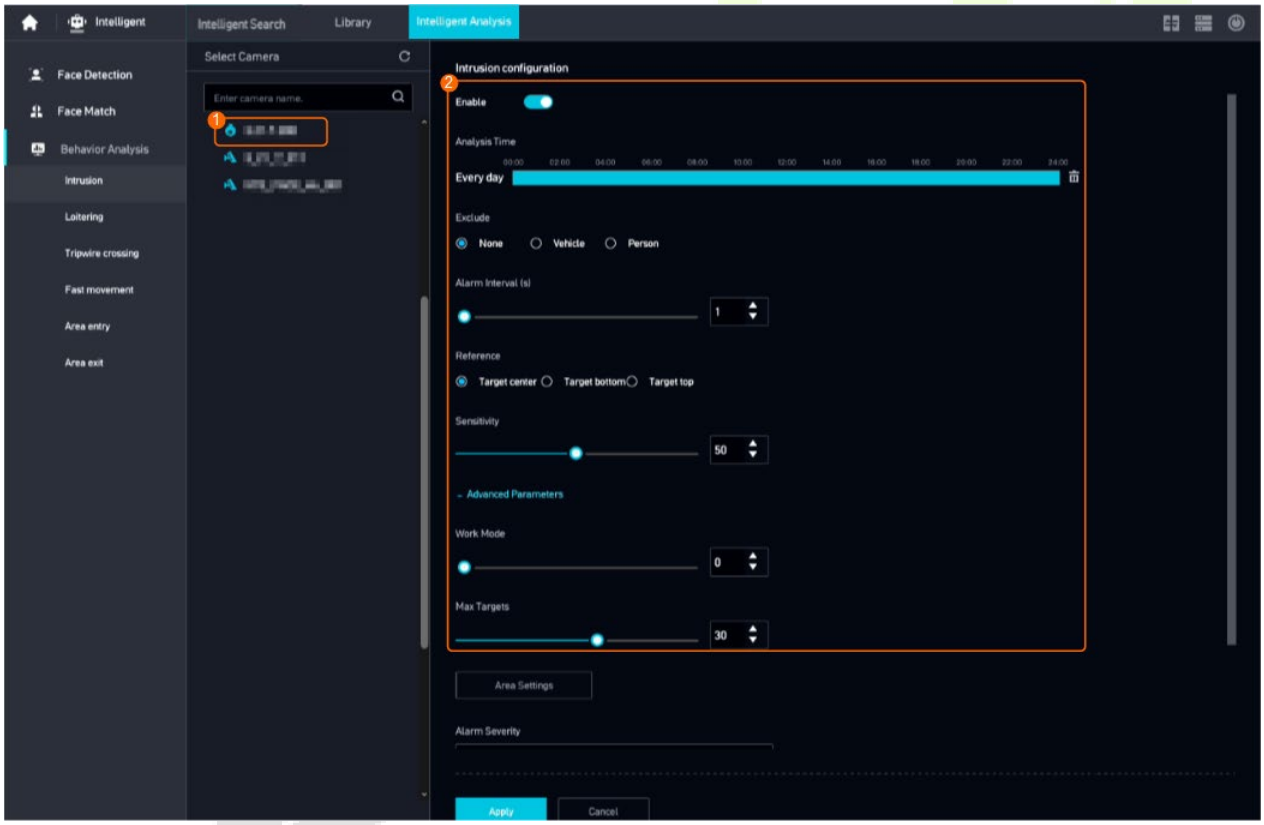
- The device analyzes video streams sent from cameras and reports an alarm when detecting intrusions.

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **Intelligent Applications**.

Step 3 Choose **Intelligent Analysis** > **Behavior Analysis** > **Intrusion**.

Step 4 Set basic intrusion detection parameters, as shown in below.

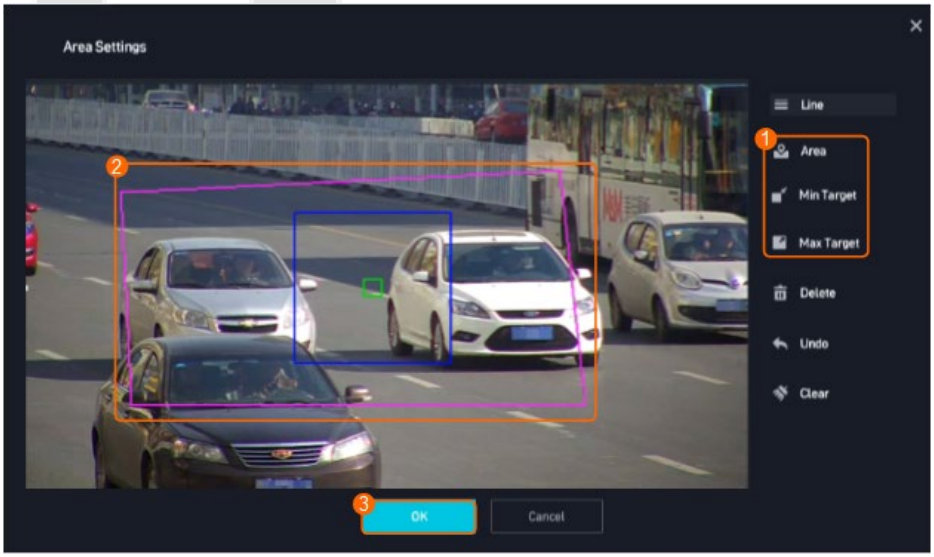


Parameter Description

Parameter	Description
Enable	Select this parameter to enable the intrusion detection alarm function.
Analysis Time	By default, intrusion detection is enabled for 24 hours a day. You can drag the time bar or manually enter a time range to adjust the intrusion detection time range.

Parameter	Description
Exclude	Select objects that are filtered out and for which no alarm is triggered as required. • None • Vehicle • Person
Alarm Interval (s)	Interval at which the camera checks for new alarms. To prevent a flood of alarms, the camera reports only one alarm even if it detects multiple alarms within the specified interval.
Reference	Set this parameter based on the site requirements. • **Target center**: The center of an object is used as the location reference. • **Target bottom**: The bottom of an object is used as the location reference. • **Target top**: The top of an object is used as the location reference.
Sensitivity	Sensitivity that is mainly used to detect the speed of a moving object. Set this parameter based on the site requirements.
Work Mode	Work mode. You can set the overall sensitivity of an analysis task. • **0**: low • **1**: medium • **2**: high • **3**: lower • **4**: lowest
Max Targets	Maximum number of objects that can be analyzed and processed in a detection area.

Step 5 Click **Area Settings** and draw a detection area, as shown in below.



Parameter Description

Parameter	Description
Area	Select polygon vertices on the video image and right-click. The system automatically connects the selected vertices to form a closed area.
Min Target	The default maximum and minimum object sizes are provided. You can click **Clear** to draw areas to configure the maximum and minimum object image sizes. An alarm is triggered only when the object size is between the minimum object size and maximum object size.
Max Target	

Step 6 (Optional) Configure intrusion detection alarm linkage, as shown in below.

Parameter Description

Parameter	Description
Alarm Severity	The default value is **Minor**. You do not need to set this parameter.
Alarm Linkage Recording	Select a camera based on the site requirements. When a camera triggers an intrusion alarm, the selected camera is linked for recording.
Snapshot	Select a camera based on the site requirements. When a camera triggers an intrusion alarm, the selected camera is linked for snapshot taking.

Step 7 Click **Apply** to complete the intrusion detection configuration.

4.4 Alarm Center

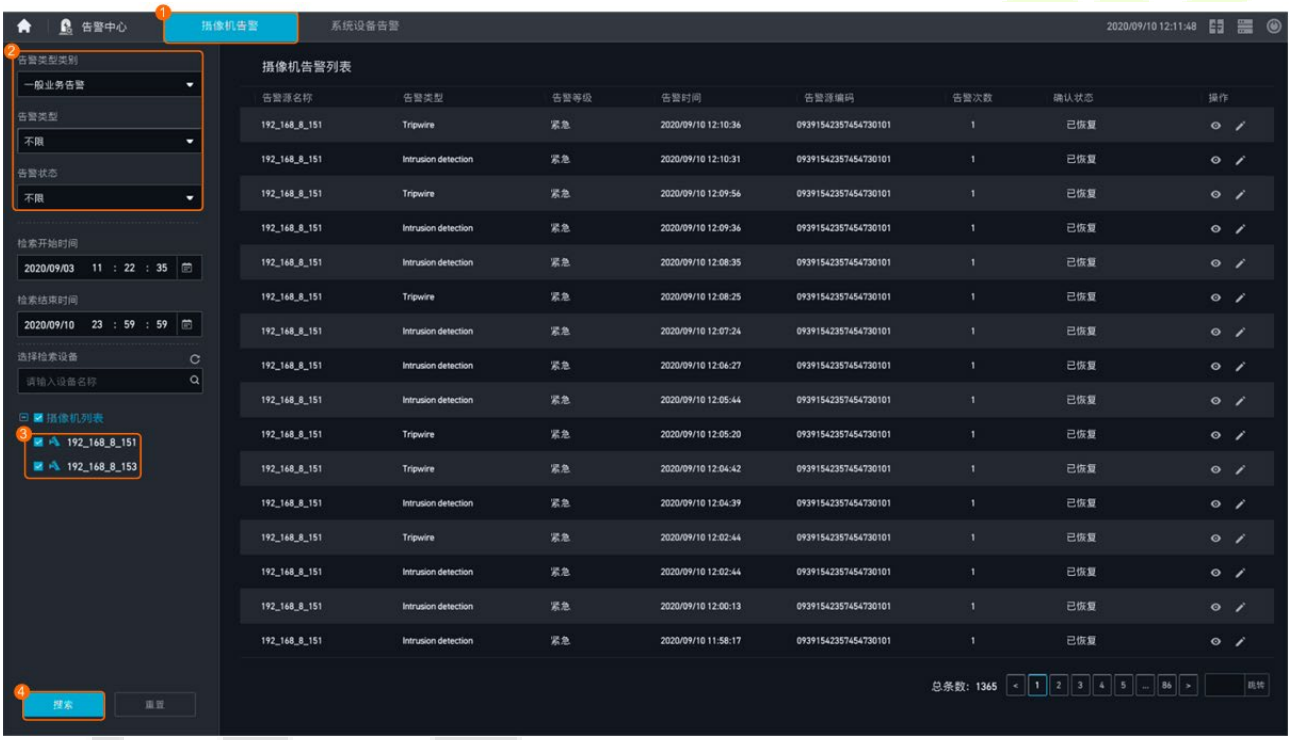
- Alarms include **Camera Alarms** and **System Device Alarms**. To search for camera alarms, access the **Camera Alarms** tab page. To search for server alarms (for example, disk and fan alarms), access the **System Device Alarms** tab page.

4.4.1 Camera Alarms

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **Alarm Center**.

Step 3 Search for camera alarms, as shown in below.



Parameter Description

Parameter	Setting
Subtype	Set this parameter as required. • Common service alarm • Behavior analysis alarm
Alarm Subtype	Select an alarm type as required, for example, **Face detected**.
Status	Set this parameter as required. • All (default value)

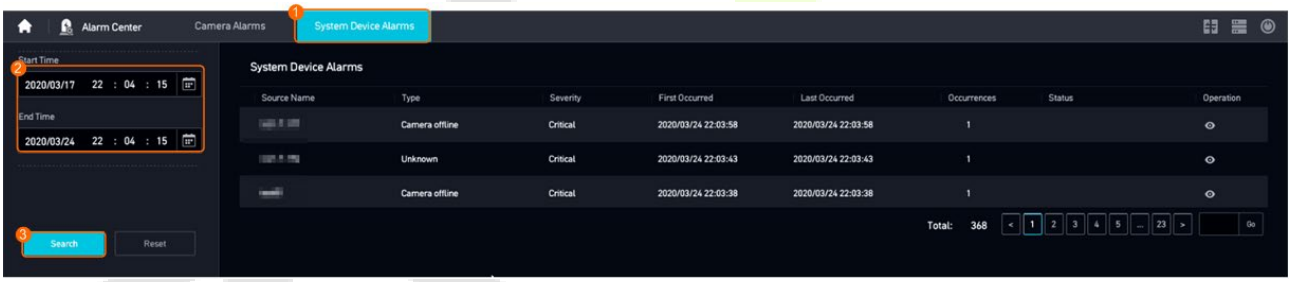
Parameter	Setting
	• Pending • To acknowledge • Acknowledged • Ignored • Cleared
Start Time/End Time	Set the time segment for searching for camera alarms as required.
	Click to view alarm details.
	Click to confirm the alarm and enter the description.

4.4.2 Viewing System Device Alarms

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **Alarm Center**.

Step 3 Search for system device alarms, as shown in below.



You can click to view alarm details.

4.5 Camera Management

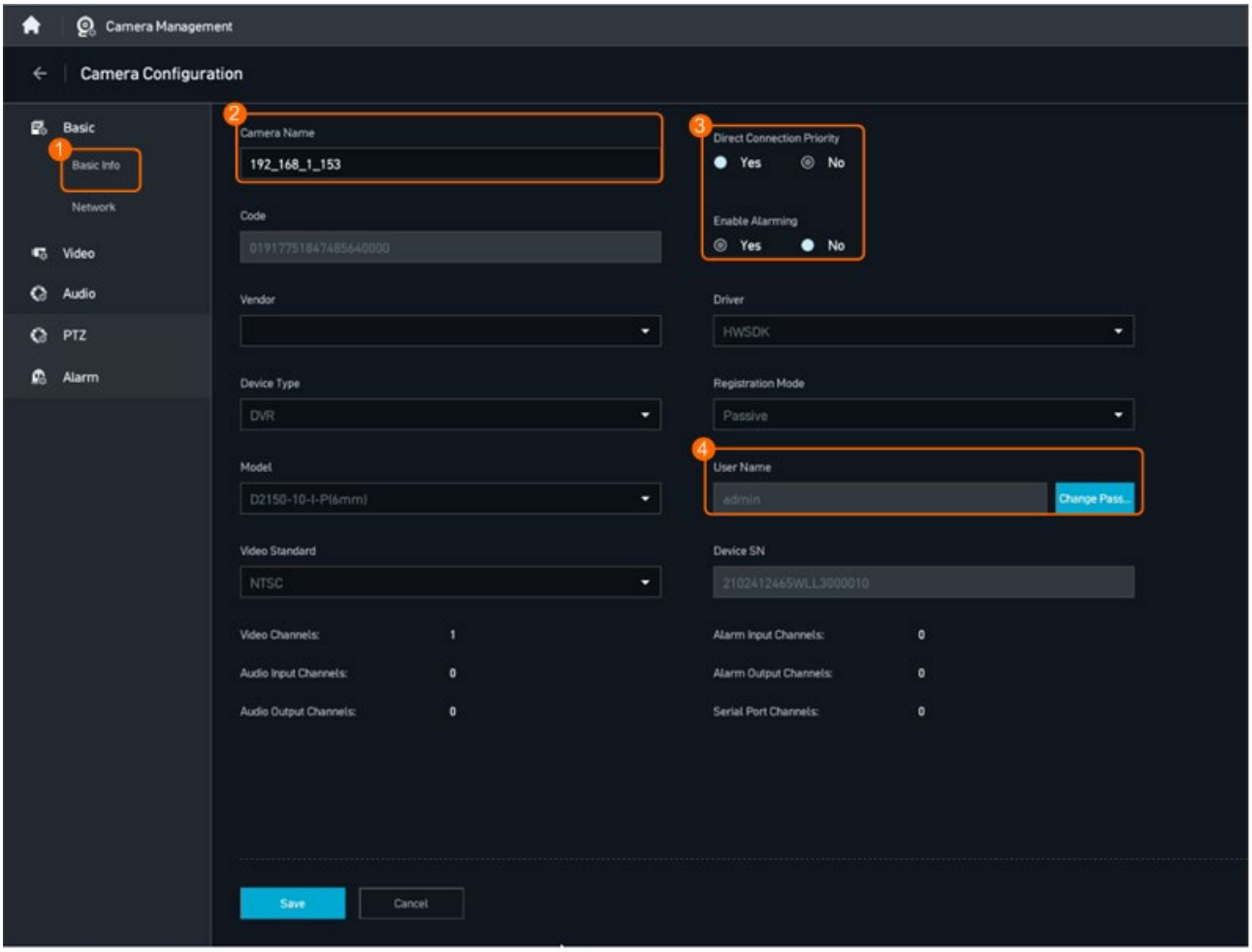
4.5.1 Configuring Basic Camera Information

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **Camera Management**.

Step 3 Click next to the specified camera.

Step 4 Modify basic camera information, as shown in below.



Parameter Description

Parameter	Description
Camera Name	Camera name. Customize the camera name.
Direct Connection Priority	In direct connection mode, the AS1700 directly obtains video streams from a camera and plays the video. Direct connection does not occupy the forwarding bandwidth of servers but has high requirements on the network quality. The default value is **No**. Set this parameter based on the site requirements.
Enable Alarming	The default value is **No**. Set this parameter based on the site requirements. Alarms on a camera can be uploaded to the device system only if you select **Yes**.
User Name/Change Password	User name and password for registering a camera with the AS1700. The settings are automatically synchronized to the camera.

4.5.2 Video Settings

4.5.2.1 Setting Intelligent Attributes for Checkpoint Cameras

- The intelligent attribute of a checkpoint camera must be the same as the actual intelligent attribute. Otherwise, snapshots taken by the checkpoint camera cannot be uploaded to the backend device.

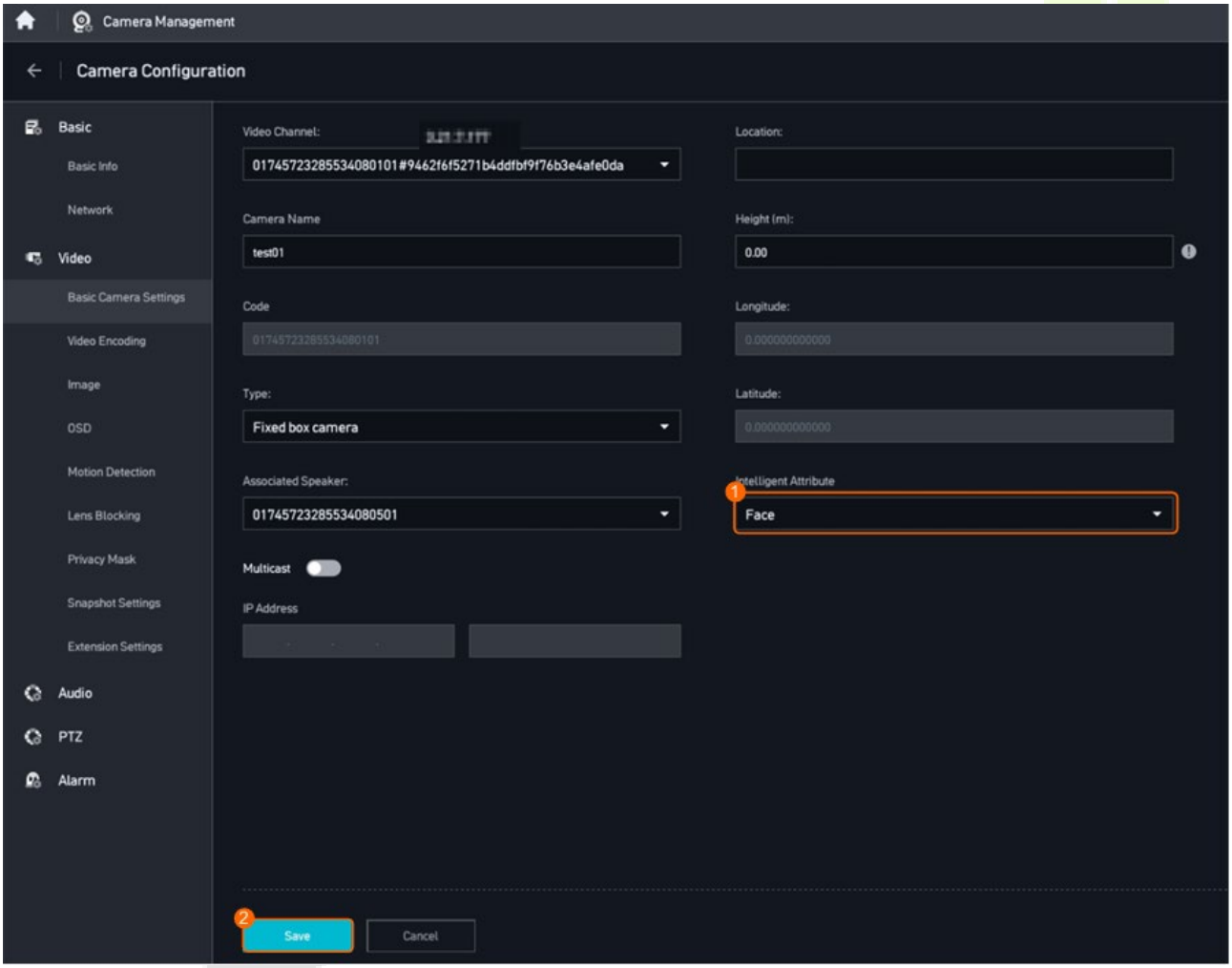
Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **Camera Management**.

Step 3 Click next to the camera for which you want to set the intelligent attribute.

Step 4 Choose **Video** > **Basic Camera Settings**.

Step 5 Set **Intelligent Attribute**, as shown in below.



Parameter Description

Parameter	Description
Intelligent Attribute	Intelligent attribute of a checkpoint camera, which must be the same as the actual intelligent attribute. Otherwise, snapshots taken by the checkpoint camera cannot be uploaded to the AS1700. • **Common**: default value. If you connect a common camera, you do not need

Parameter	Description
	to set this parameter. If you connect a checkpoint camera, set this parameter correctly. • Face • Vehicle • Object classification • Person • Face+Vehicle • Face+Person • Face+Object classification • Others

4.5.2.2 Multicast

Definition

- Live and recorded video can be played in multicast mode.

Customer Benefits

- This feature saves bandwidth resources and improves bandwidth usage for users.

Application Scenario

- When users view the live video from a camera on different clients at the same time, the multicast function is used for video distribution. This ensures good image quality and smooth video playing.

Application Limitations

- Switches must support multicast.

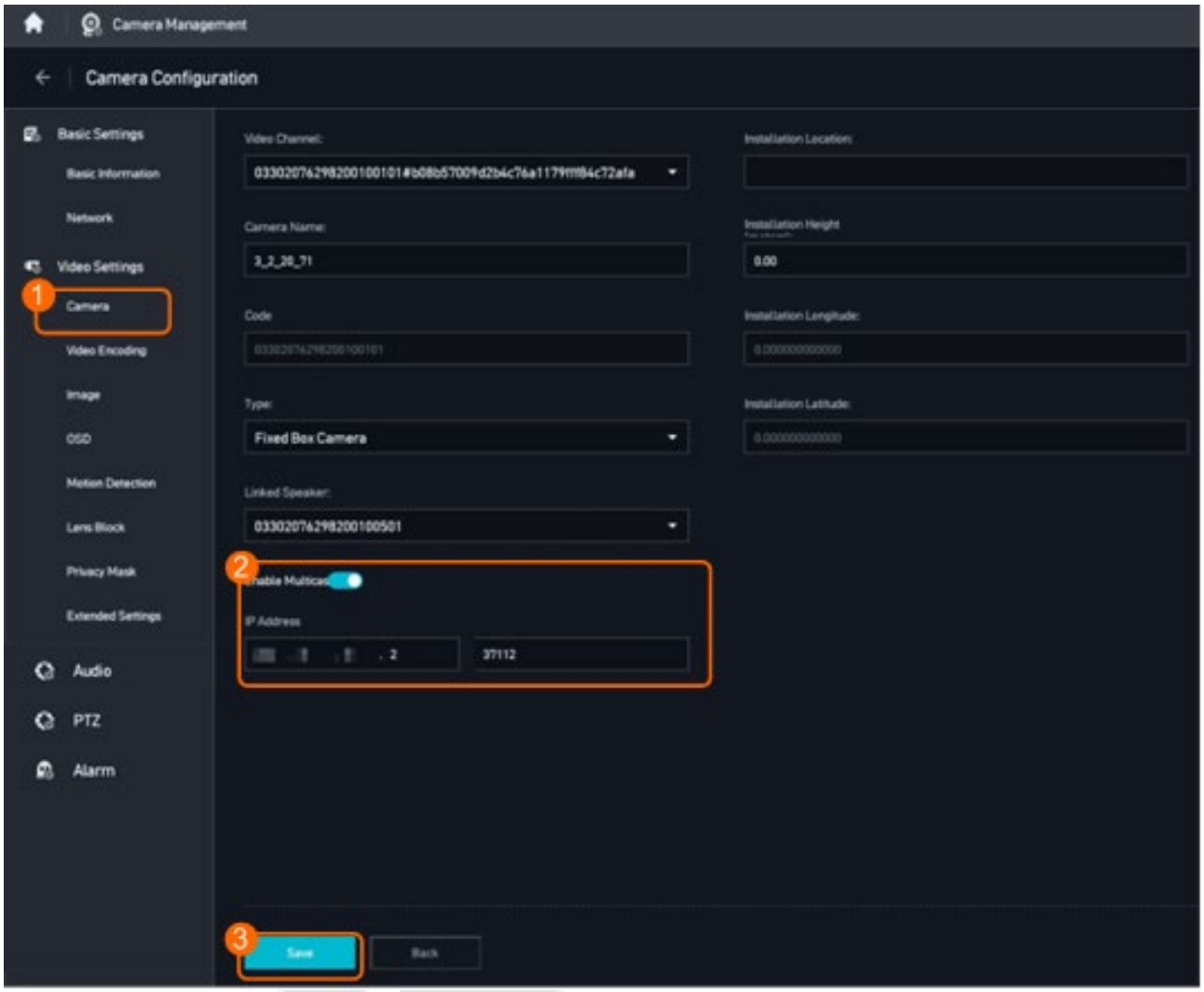
Procedure

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **Camera Management**.

Step 3 Select a specified camera and click next to the camera.

Step 4 Enable the multicast function, as shown in below.



Data Plan

Parameter	Setting Example	Restriction
IP Address	The IP address ranges from 224.0.0.0 to 239.255.255.255.	Either the multicast IP address or port number is different between every two cameras. For example, if the multicast IP address and port number of camera 1 are 224.0.0.2 and 37112 respectively, the multicast IP address and port number of camera 2 cannot be 224.0.0.2 and 37112 but can be 224.0.0.3 and 37112.
Port	The port number must be an even number ranging from 37112 to 37495.	

4.5.2.3 Bandwidth Adaptation

Definition

- The device works with cameras to detect the network bandwidth. Based on this information, the cameras dynamically adjust the bit rate to ensure smooth video.

Customer Benefits

- When the network bandwidth is unstable, this feature balances the bandwidth pressure and video effect to meet the core requirements of users.

Application Scenario

- If a user has high requirements on video smoothness but the network bandwidth is unstable, cameras automatically degrade the image quality to ensure smooth video playing.

Application Limitations

- This feature is supported only when cameras are connected to the device but not in scenarios where cameras are directly connected to the client.

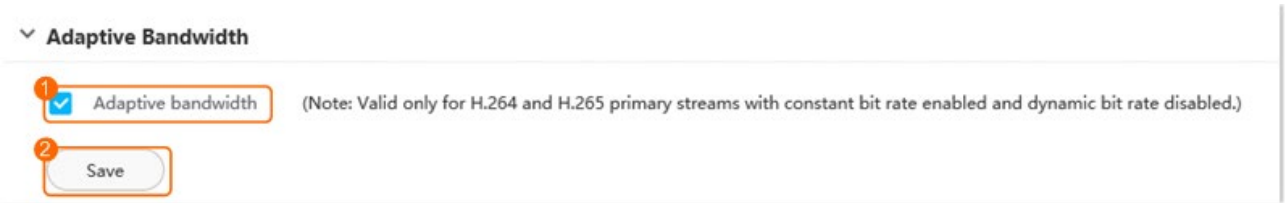
Context

- With the bandwidth adaptive function enabled, the camera will use an appropriate bit rate that best suits the current network conditions to transfer video images. This approach ensures the image quality.
- This function is valid only when the following conditions are met:
  - The stream type is set to Primary stream.
  - The encoding protocol is set to H264 or H265.
  - The bit rate type is set to Constant bit rate.
  - The dynamic bit rate is disabled.

Procedure

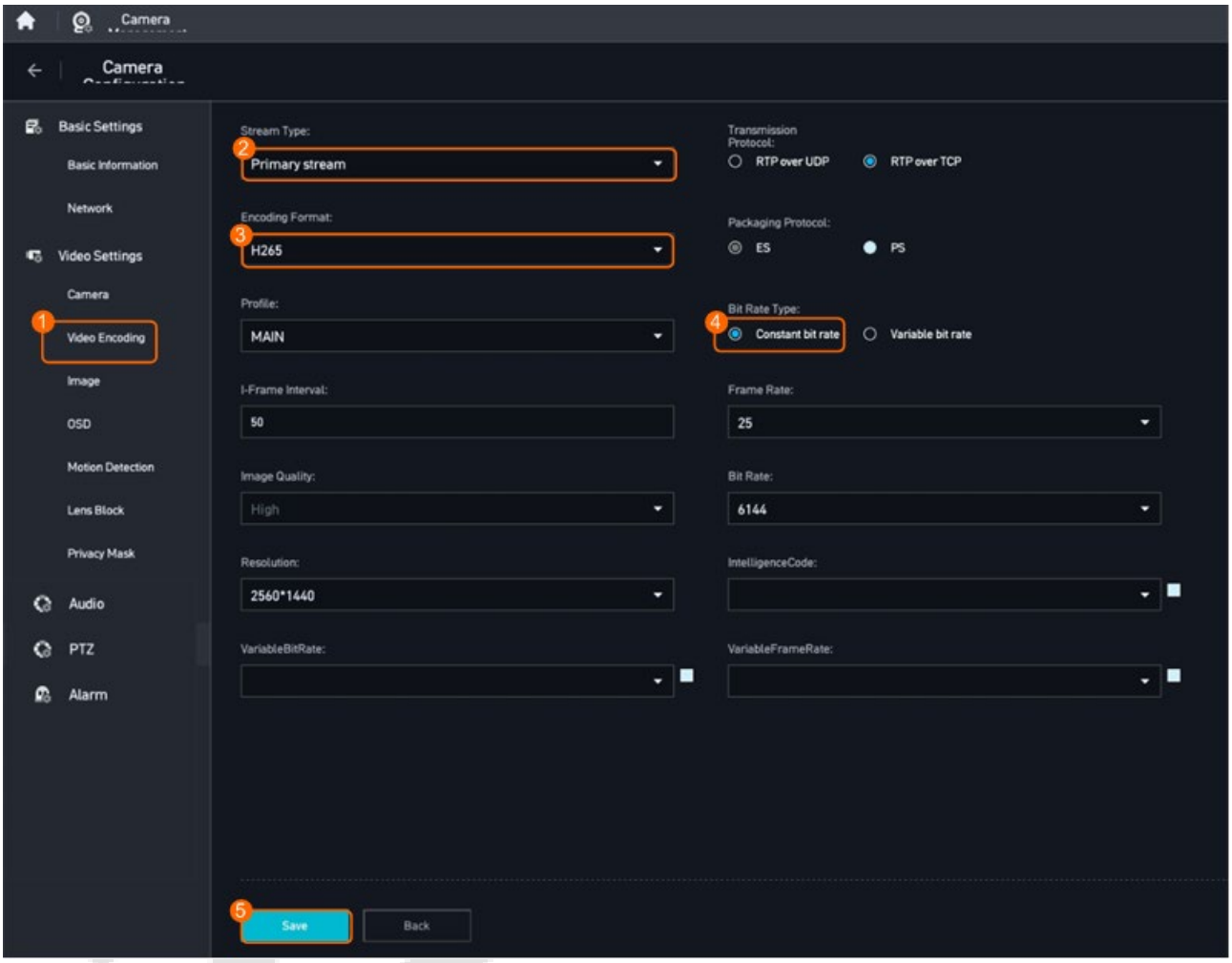
Step 1 Enable the bandwidth adaptation function on the camera.

1) Log in to the camera web system as the **admin** user.
2) Choose **Settings** > **Network** > **Intelligent Acceleration** > **Adaptive Bandwidth**.
3) Enable bandwidth adaptation, as shown in below.



Step 2 Set bandwidth adaptation parameters on the AS1700 side.

1) Log in to the LDU as the **admin** user.
2) Right-click the desktop and choose **Camera Management**.
3) Select a specified camera and click next to the camera.
4) Configure a constant bit rate, as shown in below.



Parameter Description

Parameter	Description
Stream Type	• Primary stream • Secondary stream Select **Primary stream**.
Encoding Format	• H.264 • H.265 • MJPEG Select **H264** or **H256**.

Parameter	Description
Constant bit rate	Constant bit rate indicates that the rate at which a codec's output data should be consumed is stable. If the bit rate is incorrectly configured for images with fast encoding and compression speed but great dynamic changes, the images will be unclear.
Variable bit rate	The bit rate varies depending on the image complexity to ensure that large dynamic images are clear. However, the compression speed is low. The bit rate is low if the image is simple or static.

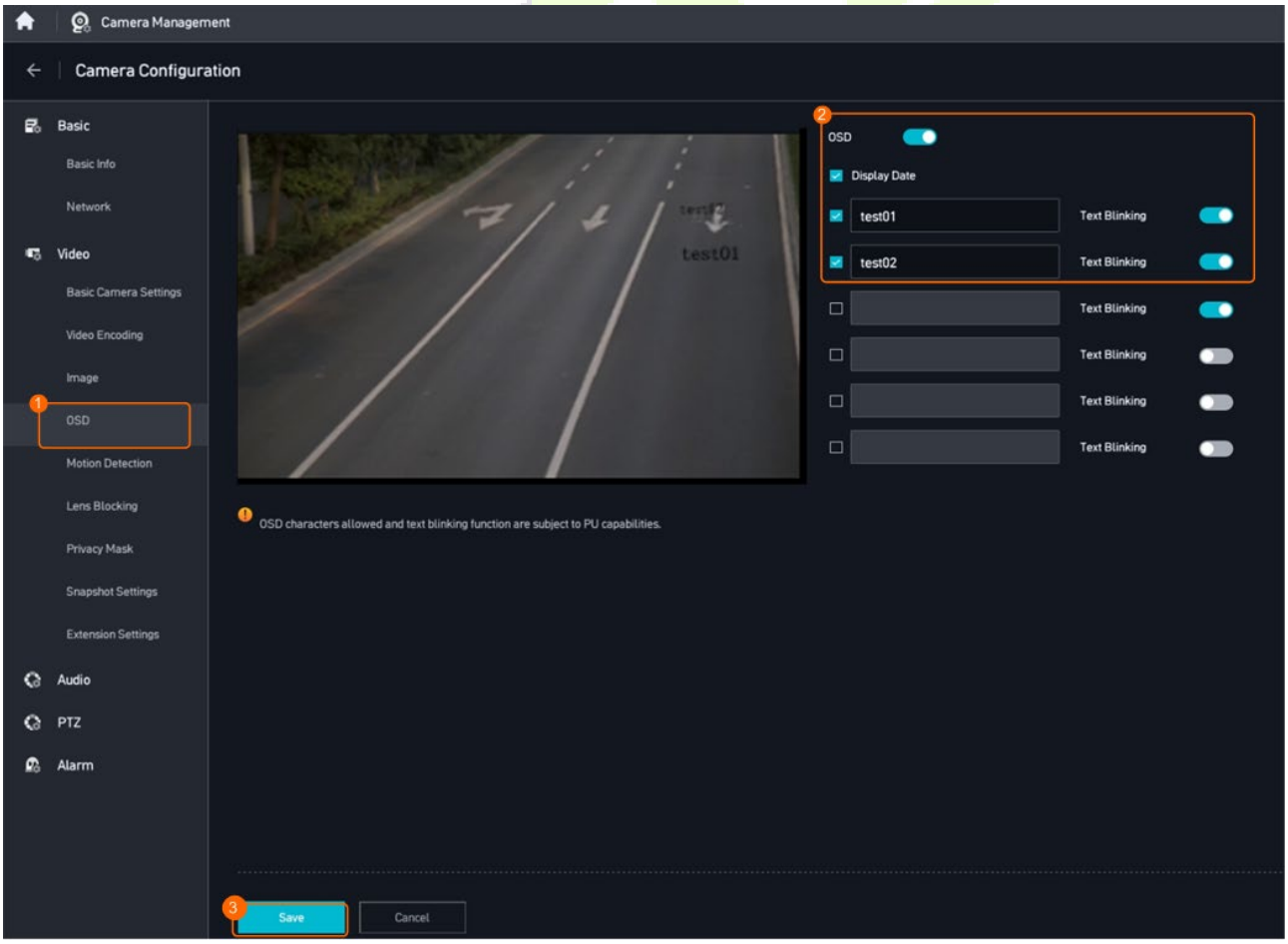
4.5.2.4 Configuring the OSD Text for a Camera

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **Camera Management**.

Step 3 Click next to the specified camera.

Step 4 Configure the OSD text for a camera, as shown in below.



4.5.2.5 Motion Detection

- The system automatically generates an alarm when a motion is detected in a specified surveillance area. Surveillance personnel can view the video image to identify harmful objects and take necessary actions.

Scenario Description

- You can configure motion detection on the LDU or camera web page.

  This section uses the LDU as an example. For details about how to configure motion detection on the camera web page, see the corresponding camera documentation.

- If a camera is connected to the AS1700 through ONVIF, motion detection cannot be enabled for the camera. Therefore, it is recommended that cameras be connected to the AS1700 through HWSDK.

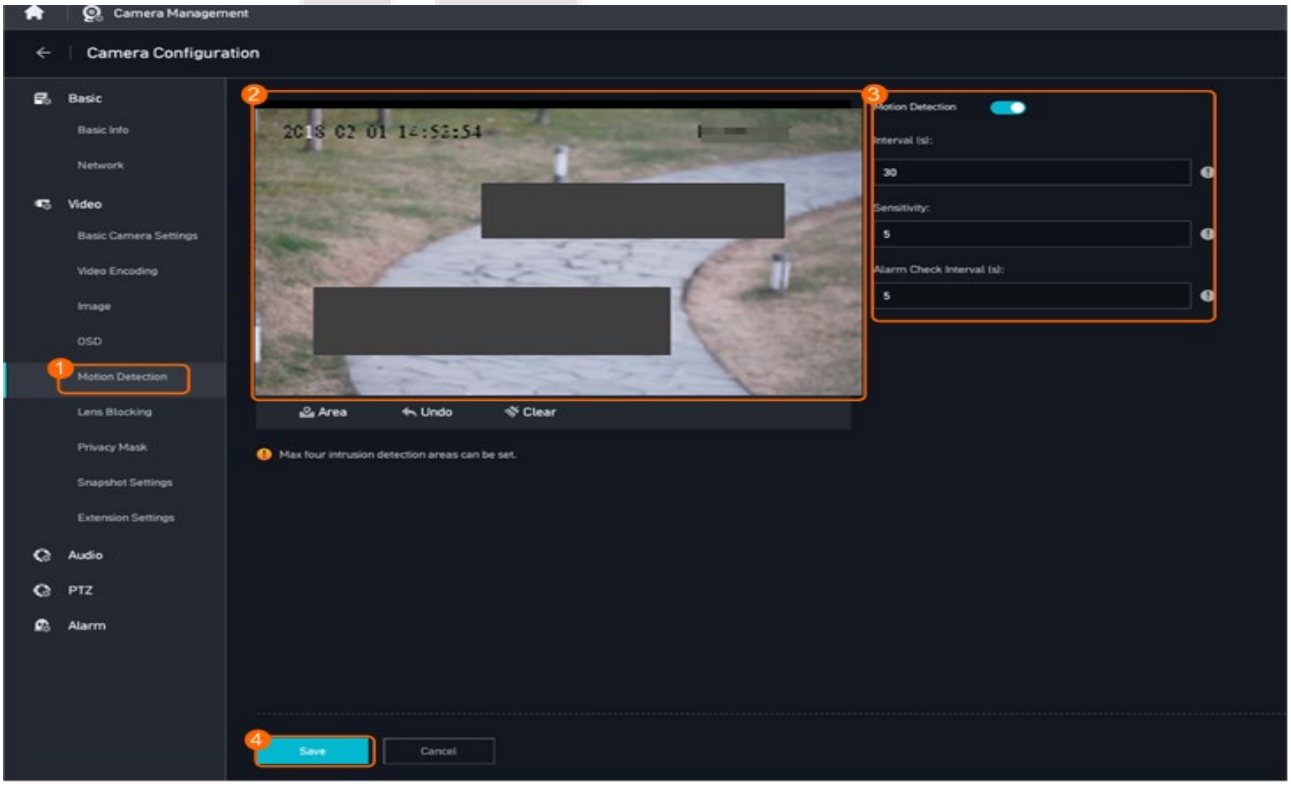
Procedure

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **Camera Management**.

Step 3 Click ⚙ next to the specified camera.

Step 4 Configure motion detection, as shown in below.



Parameter Description

Parameter	Description
Motion Detection Interval (s)	Interval for detecting object motions.
Motion Detection Sensitivity	Detection sensitivity. There are five sensitivity levels ranging from 1 (the lowest level) to 5 (the highest level). If a higher sensitivity level is used, motions that are difficult to detect can be detected.
Alarm Check Interval (s)	Interval at which the camera detects object motion. If a motion is detected, the camera reports an alarm. If an object keeps moving in the surveillance range of a camera, only one alarm is reported during each motion detection interval.

NOTE:

- The minimum length of a selected area is 50 pixels by default, and the total length is 480 pixels. If the distance from the start position of a selected area to the right border of the surveillance image is less than the minimum length, the area cannot be selected.

4.5.2.6 Configuring Privacy Mask

Context

- You can select a maximum of five areas on the video image and enable privacy mask so that these areas will be masked.

Prerequisites

- You have rotated a camera to the specified position (to monitor an area for which privacy mask needs to be enabled). For details, see 7.2.3Configuring Preset Positions and the Home Position.

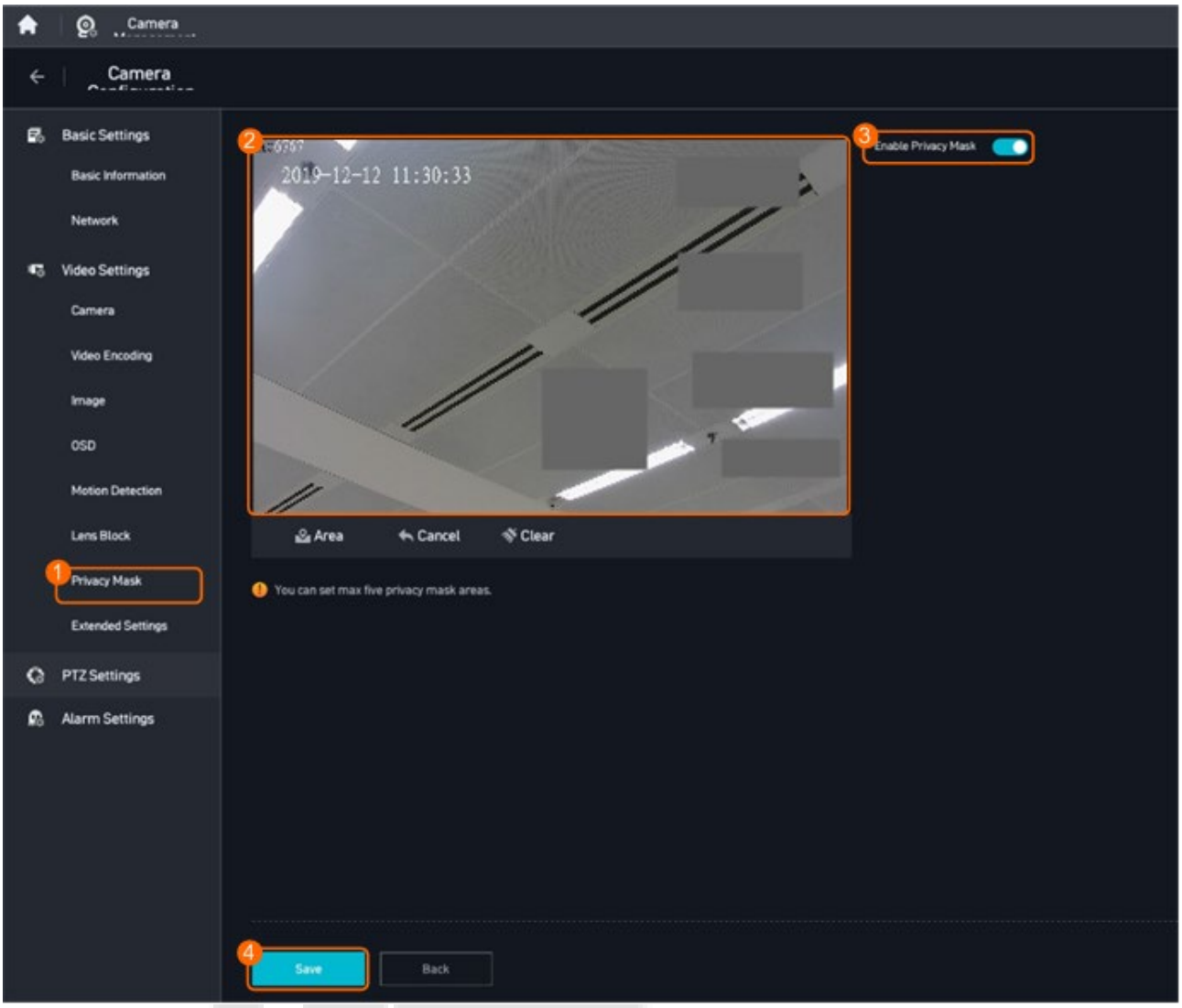
Procedure

Step 1 Log in to the LDU as the admin user.

Step 2 Right-click on the desktop and choose **Camera Management**.

Step 3 Click ⚙ next to the specified camera.

Step 4 Configure privacy mask, as shown in below.



NOTE:

- The minimum length of a selected area is 50 pixels by default, and the total length is 480 pixels. If the distance from the start position of a selected area to the right border of the surveillance image is less than the minimum length, the area cannot be selected.
- After privacy mask is enabled, users cannot view live video in the privacy masked area. The privacy masked area is fixed. It does not change when you rotate the camera.

4.5.2.7 Lens Blocking Detection

- The system automatically generates an alarm when the camera lens is blocked by an object in a specified area. Surveillance personnel can view the video image to identify harmful objects and take necessary actions.

Scenario Description

- You can configure lens blocking detection on the LDU or camera web page.

  This section uses the LDU as an example. For details about how to configure lens blocking detection on the camera web page, see the corresponding camera documentation.

- If a camera is connected to the AS1700 through ONVIF, the lens blocking detection function cannot be enabled for the camera. Therefore, it is recommended that cameras be connected to the AS1700 through HWSDK.

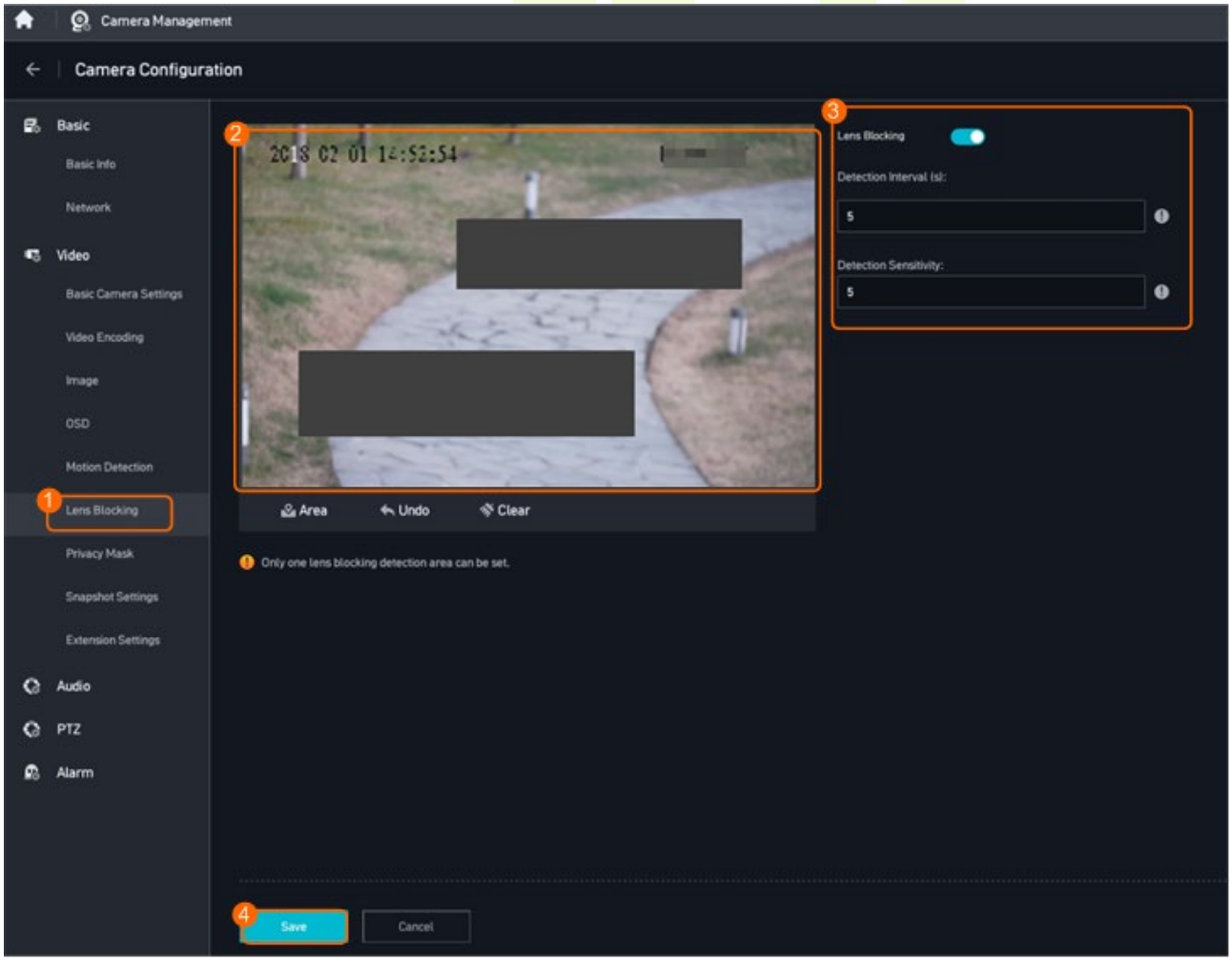
Procedure

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **Camera Management**.

Step 3 Click ⚙ next to the specified camera.

Step 4 Configure lens blocking detection, as shown in below.



Parameter Description

Parameter	Description
Lens Blocking Detection Interval (s)	The system checks for new lens blocking alarms at a specified interval.
Detection Sensitivity	Detection sensitivity. There are five sensitivity levels ranging from 1 (the lowest level) to 5 (the highest level). With a higher sensitivity, the camera can generate alarms when the lens is blocked by an object with a smaller size and brighter luminance.

NOTE:

- The minimum length of a selected area is 50 pixels by default, and the total length is 480 pixels. If the distance from the start position of a selected area to the right border of the surveillance image is less than the minimum length, the area cannot be selected.

4.5.2.8 FEC

Definition

- FEC-enabled media transmission is supported, ensuring that the video is played smoothly even with a 5% packet loss. The FEC parameters are configurable.

Customer Benefits

- When packet loss occurs on the network, this feature balances the bandwidth pressure and video effect to meet the core requirements of users.

Application Scenario

- If a user has high requirements on video smoothness but packet loss occurs on the network, cameras automatically degrade the image quality to ensure smooth video playing.

Application Limitations

- FEC and media security cannot be enabled at the same time.
- This feature is supported only when cameras are connected to the SerilgI1324 but not in scenarios where cameras are directly connected to the client.
- This feature takes effect only when UDP is used for transmission.

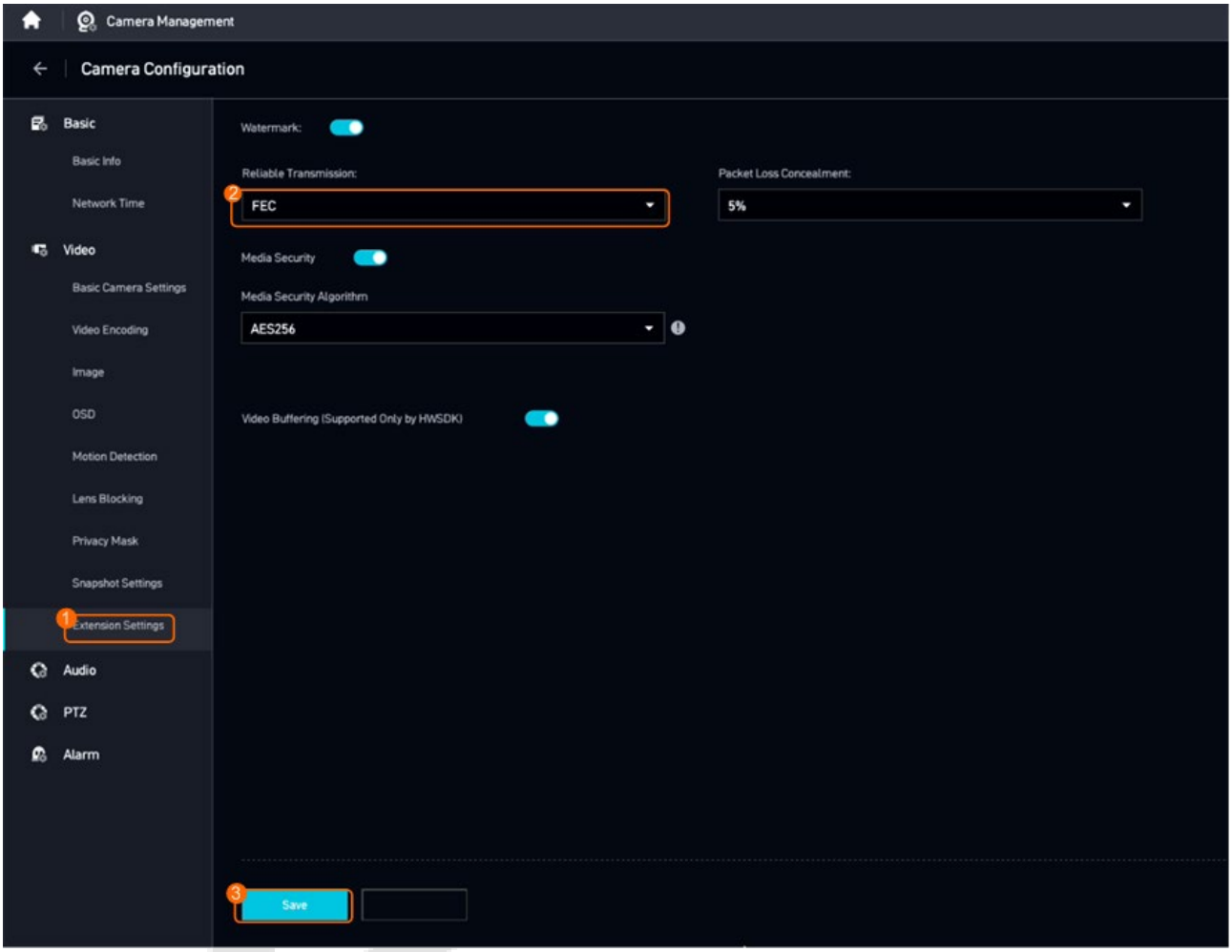
Procedure

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **Camera Management**.

Step 3 Select a specified camera and click next to the camera.

Step 4 Set FEC parameters, as shown in below.



Parameter Description

Parameter	Description
Reliable Transmission	Select **FEC**.
Packet Loss Concealment	Select a packet loss concealment rate based on the site requirements. The value ranges from 1% to 5%. In this example, the value is **5%**.

4.5.2.9 Video Buffering

Definition

- A camera can automatically enable local storage when the network between the device and camera is disconnected, and automatically send data to the device when the network recovers.

Customer Benefits

- This feature avoids recording and checkpoint data loss in case of network disconnections, improving system reliability and video and image storage continuity.

Application Scenario

- When the network is disconnected, the media streams and checkpoint data generated by cameras are stored in the SD card of the cameras. After the network recovers, the data is automatically uploaded to the device through the video buffering function.

Application Limitations

- The detected network disconnection time may be later than the actual network disconnection time, so the video shot within this interval may be lost.
- When the SD card of a camera is full, the earliest recordings will be overwritten cyclically.
- The video buffering channels account for 5% of the total camera access channels. The speed for downloading buffered video is 1x.

Context

- When the network is disconnected, cameras can temporarily store the scheduled recordings locally based on the server recording plan. To ensure video integrity, users can use the video buffering function. After the network is recovered, the platform sends a video buffering request to the cameras, and the cameras send the stored video to the server.

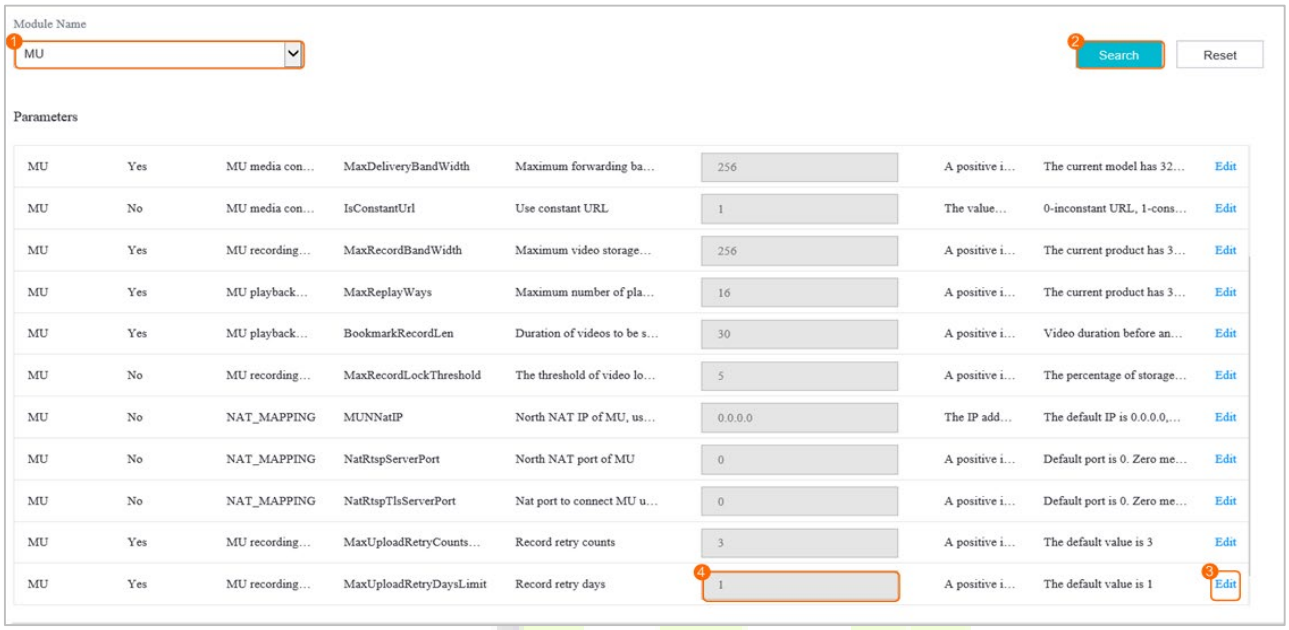
Prerequisites

- Cameras are equipped with SD cards, and can execute recording tasks properly.
- Time has been synchronized from the server to the cameras.

Procedure

Step 1 Set video buffering parameters.

1. Choose **Maintenance** > **Unified Configuration**.
2. Configure the number of retry days upon video supplementation failure, as shown in below.



Parameter Description

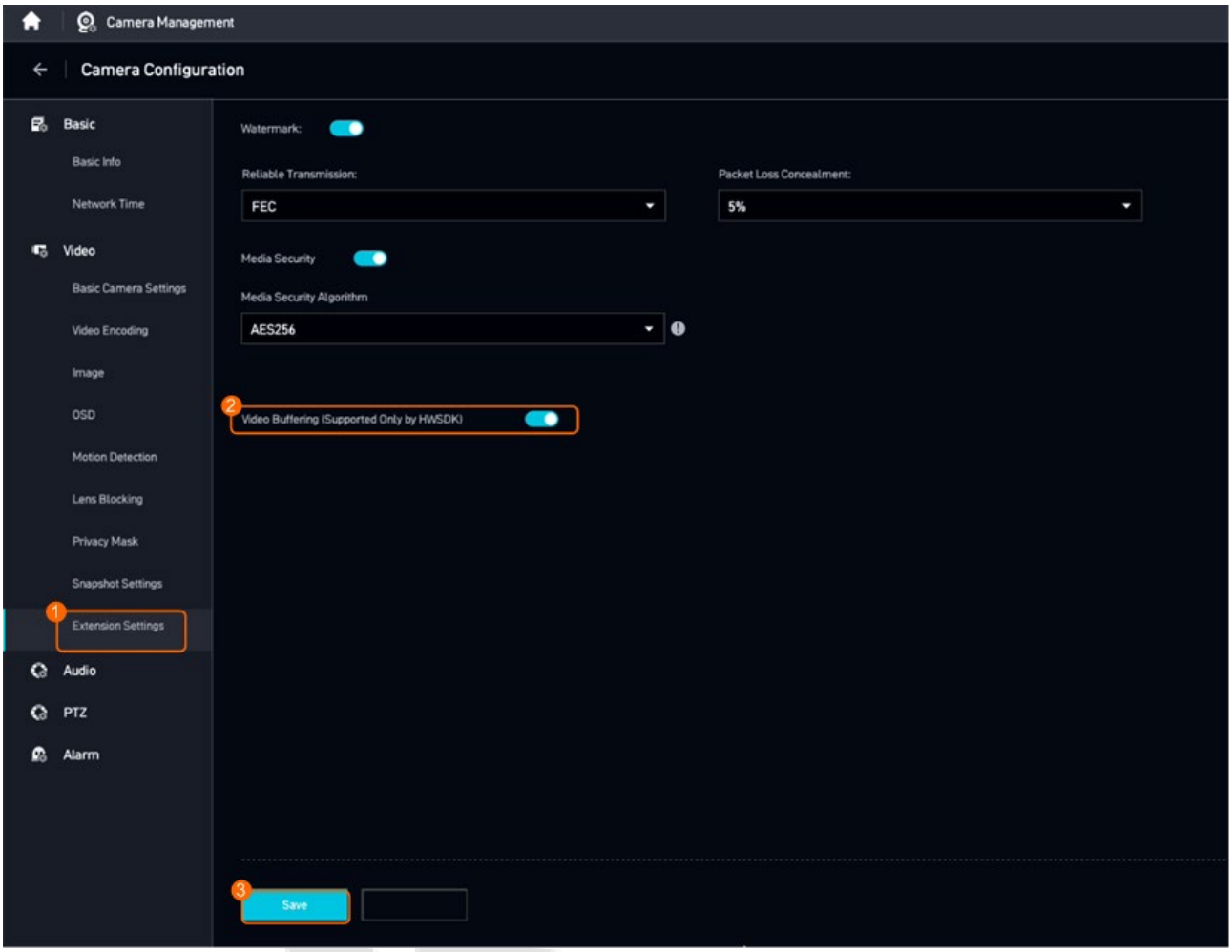
Parameter	Description
MaxUploadRetryCountsLimit	Maximum number of retries to upload buffered video. The value range is [3,120]. For example, set this parameter to **4**. After the camera goes online again, the system triggers video buffering. If video buffering fails for four consecutive times, the system skips the current recording and proceeds with video buffering of the next recording.
MaxUploadRetryDaysLimit	Maximum number of days to retry uploading buffered video. The value range is [1,180]. For example, set this parameter to **5**. When the camera goes online again, the system sends a request to upload buffered recordings of the last three days.

3. Set **MaxUploadRetryCountsLimit** by referring to Step 1.

Step 2 Enable the video buffering function.

1. Log in to the LDU as the **admin** user.
2. Right-click on the desktop and choose **Camera Management**.
3. Select a specified camera and click next to the camera.

4. Enable video buffering, as shown in below.



4.6 System Management

On the Main Menu, click **System Management** to set the related system parameters in order to optimize the performance of the device.

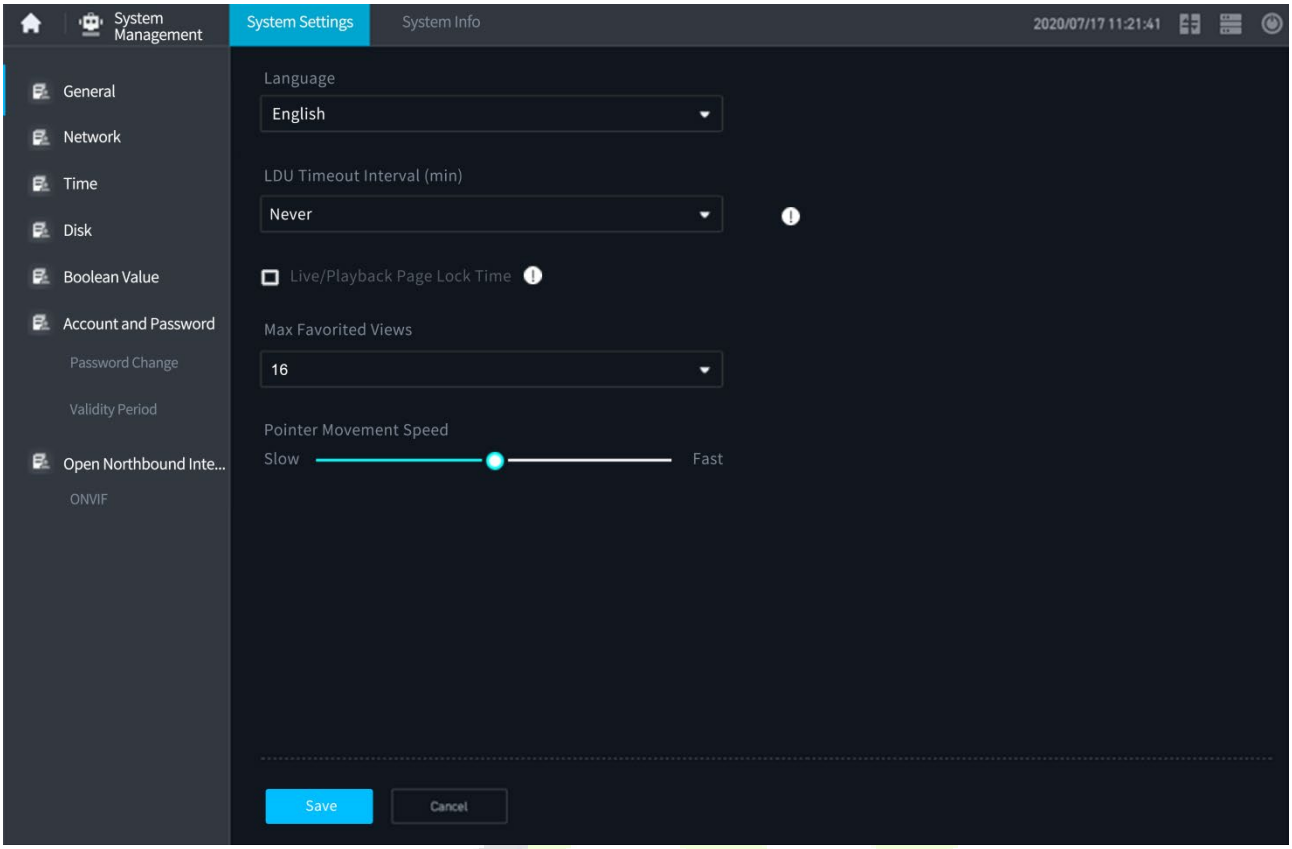
4.6.1 General Settings

Procedure

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **System Management**.

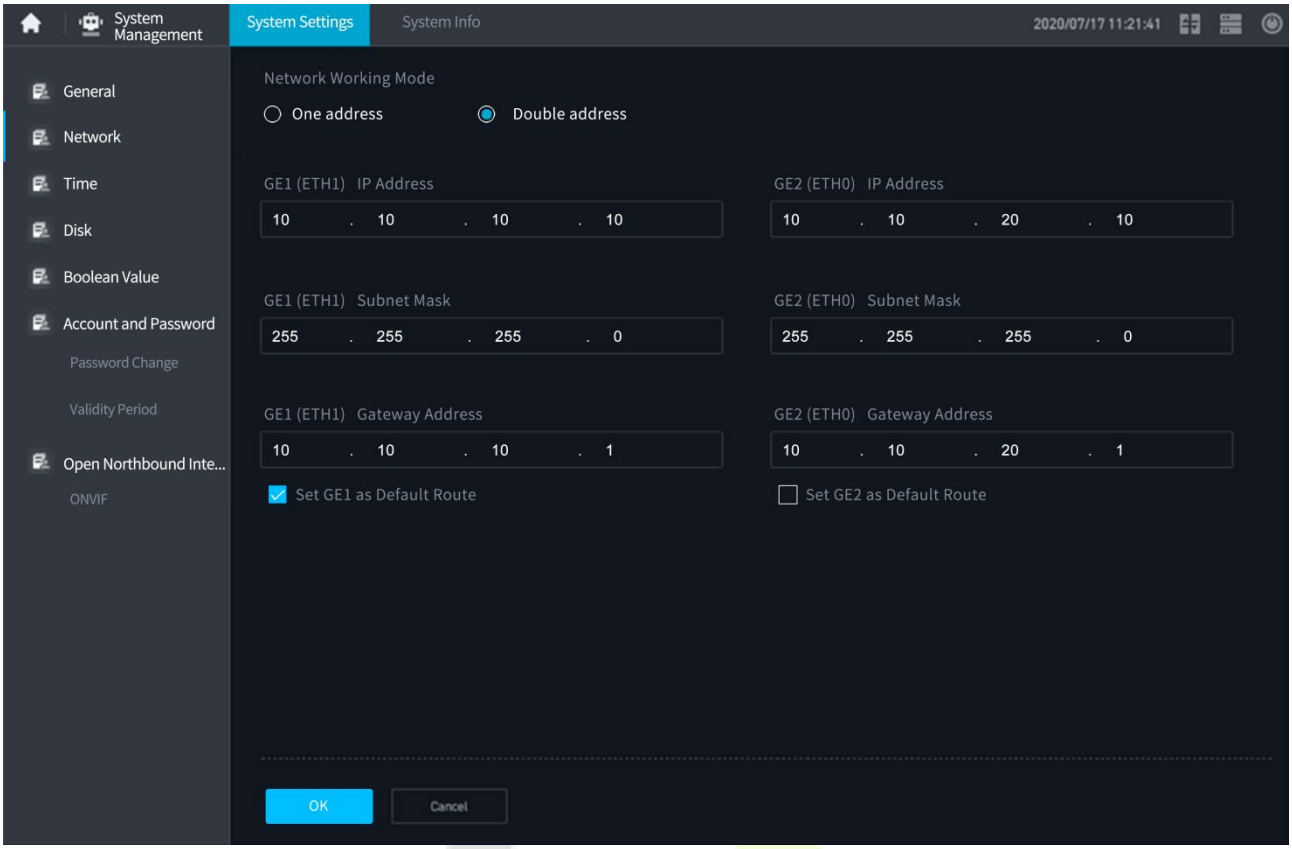
Step 3 Choose **General** to set related parameters.



Parameter Description

Parameter	Description
Language	The language of the GUI is displayed. The LDU supports two languages, "Chinese" and "English".
LDU Timeout Interval (min)	When the non-operating time of the LDU exceeds the set value, it will automatically exit to the login interface. When set to "Never", the screen lock will be cancelled.
Live/Playback Page Lock Time	• This parameter is selected. If no operation is performed within the specified period, the system automatically locks the screen, but the live video viewing or recording playback continues. You can click any area on the GUI and enter the login password to unlock the screen. • This parameter is not selected. If no operation is performed within the specified period, the system automatically redirects you to the login page.
Max Favorited Views	The LDU supports 0 to 16 favorited layouts.
Pointer Movement Speed	Change the pointer movement speed.

4.6.2 Network Settings



Parameter Description

Parameter	Description
Network Working Mode	One address mode • If the intelligent edge device, cameras, and surveillance client are on the same network, select the one address mode. Double address mode • If the intelligent edge device, cameras, and surveillance client are on different networks, select the double address mode. – Cameras can be connected to the AS1700 through the GE2 network port, which is used for southbound connection. – The VMS is connected to the AS1700 only through the GE1 network port, which is used for northbound connection.
IP Address	The default IP address is **192.168.3.111**. Can be modified according to the network availability.
Subnet Mask	The default Subnet Mask is 255.255.255.0. Can be modified according to the network availability.
Gateway	The default Gateway address is 0.0.0.0. Can be modified according to the network availability.

4.6.3 Time Settings

4.6.3.1 Configuring Time Synchronization for AS1700 with the NTP Server

Procedure

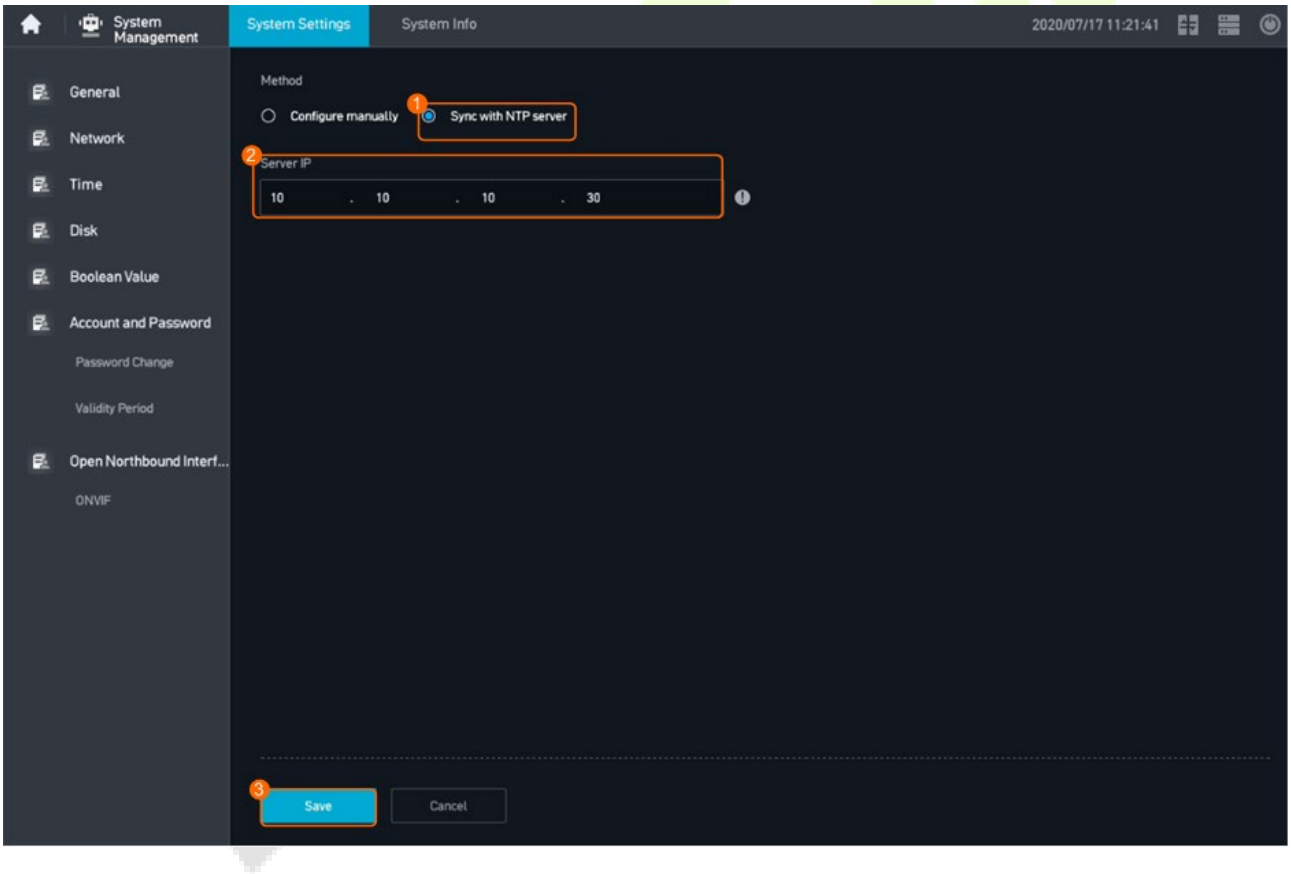
Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop to access the main menu.

Step 3 Choose **System Management** > **Time Configuration**.

Step 4 Configure time information of the server.

1) If an NTP server is configured onsite, synchronize the time from the NTP server, as shown in below.

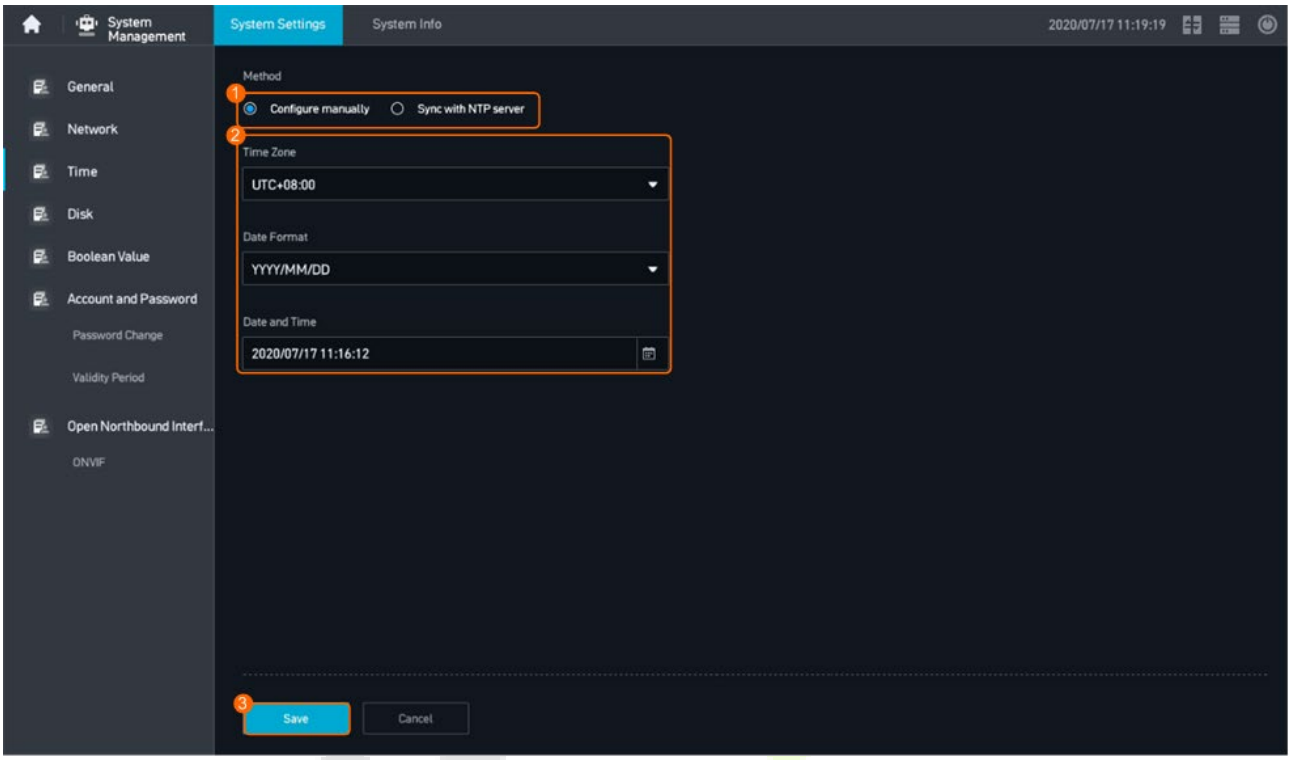


Parameter Description

Parameter	Description
Time Configuration Mode	• If no NTP server is configured onsite, select **Configure manually**. • If the NTP server is configured onsite, select **Sync with NTP server**.

Parameter	Description
ServerIP	Enter the IP address of the NTP server based on the site requirements.

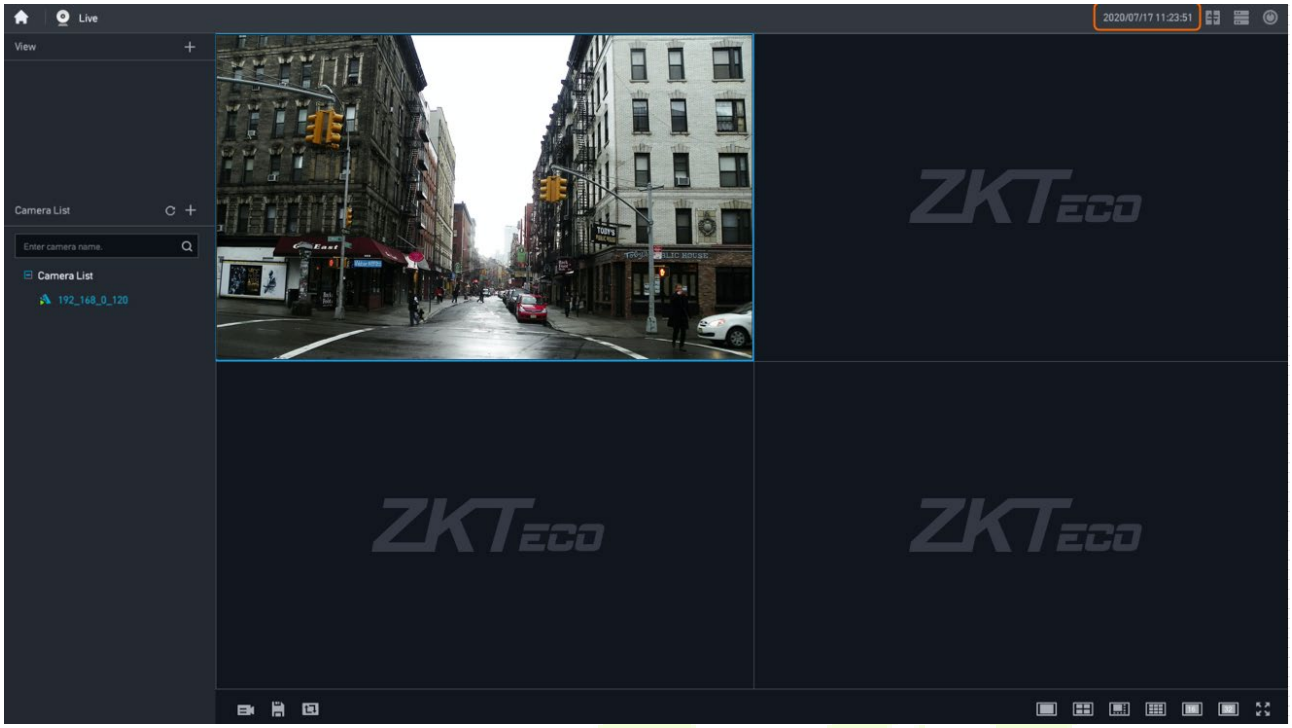
2) If no NTP server is configured, manually configure the server time, as shown in below.



Parameter Description

Parameter	Description
Time Configuration Mode	• If no NTP server is configured onsite, select **Configure manually**. • If the NTP server is configured onsite, select **Sync with NTP server**.
Time Zone	Set the time parameters based on the actual requirements.
Date Format	
Date and Time	

Step 5 View the current date and time on the LDU, as shown in below.



Step 6 Check whether the LDU time is consistent with the NTP server time.

If the current LDU time is different from the NTP server time, reconfigure NTP time synchronization for the LDU.

4.6.4 Disk Settings

4.6.4.1 Hard Disk Expansion

Scenario Description

Scenario	Description
RAID 5 mode	Add hard disks to the existing RAID 5 group. For example, if the RAID 5 group contains five hard disks, add one more hard disk so that the number of hard disks in the RAID 5 group is increased to six. For RAID 5 capacity expansion, you need to add hard disks to the current RAID 5 instead of configuring new RAID 5 groups.
Non-RAID mode	Add hard disks based on the number of existing non-RAID hard disks. For example, if the current system contains five non-RAID hard disks, add one more hard disk. Therefore, the number of non-RAID hard disks is increased to six. In non-RAID mode, if there are three or more hard disks, the non-RAID mode can be switched to RAID 5 mode. The RAID 5 mode is more reliable than the non-RAID

Scenario	Description
	mode. **Switching the hard disk mode will lose all recording data on the original hard disks. Therefore, you must obtain the user's consent before switching the hard disk mode.** For details about how to switch the hard disk mode, see 4.6.4.2 Switching the Disk Mode.

Principles

- **RAID 5 capacity expansion mechanism**

a. A hard disk is added to the original RAID group, as shown in Figure 1.

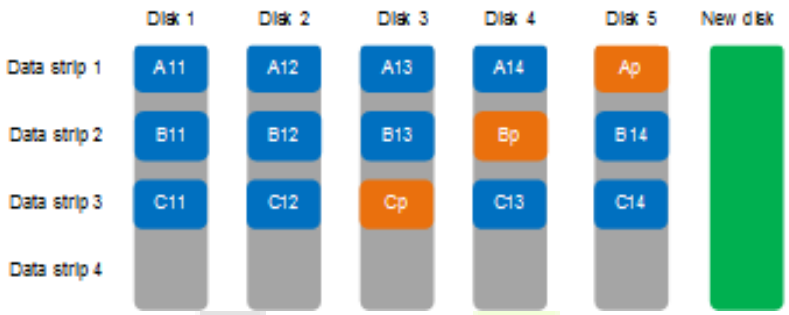


Figure 1 Adding a hard disk to the RAID group

b. New recording data is stored in the same data strip on all hard disks, as shown in Figure 2.

Recording data needs to be stored in the same data strip on all hard disks. Therefore, data strips 1, 2, and 3 of the new hard disk are not used.

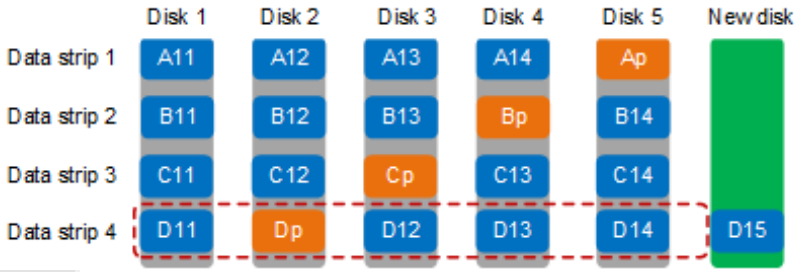


Figure 2 Recording storage

c. When the hard disk space is used up and the overwriting condition is triggered, the system reclaims the recording data in data strips 1, 2, and 3 in sequence. New recording data is stored in data strips 1, 2, and 3 in sequence, as shown in Figure 3.

The space of the new hard disk is utilized until all recording data in data strips 1, 2, and 3 is overwritten by new data.

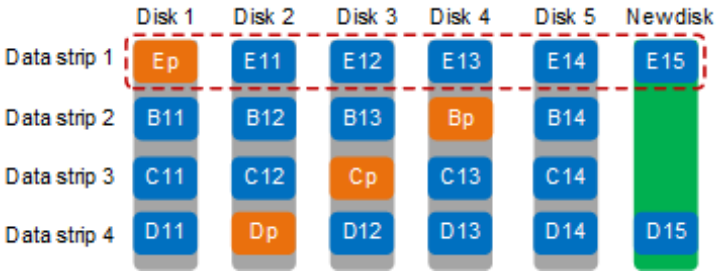


Figure 3 Overwriting when the hard disk space is used up

- **Non-RAID capacity expansion mechanism**

a. A hard disk is added to the original non-RAID group, as shown in Figure 4.

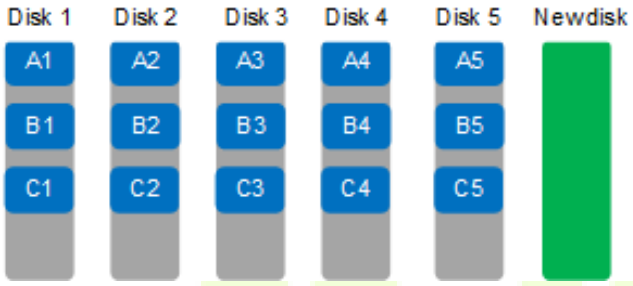


Figure 4. Adding a hard disk to the non-RAID group

b. New recording data is preferentially stored in the new hard disk until the available space of the new hard disk is the same as that of the original hard disks, as shown in Figure 5.

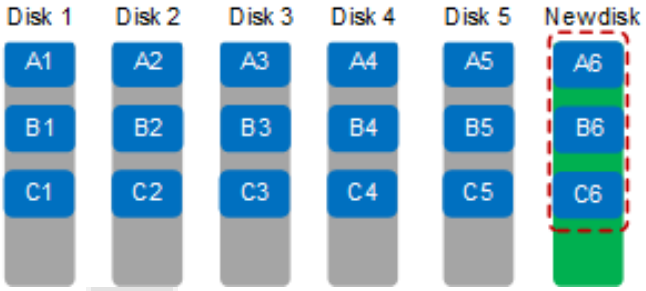


Figure 5 Recording storage

c. New recording data is stored in each hard disk in sequence, as shown in Figure 6.

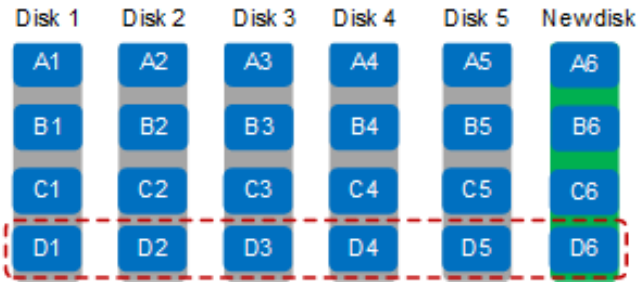


Figure 6 Recording storage

Prerequisites

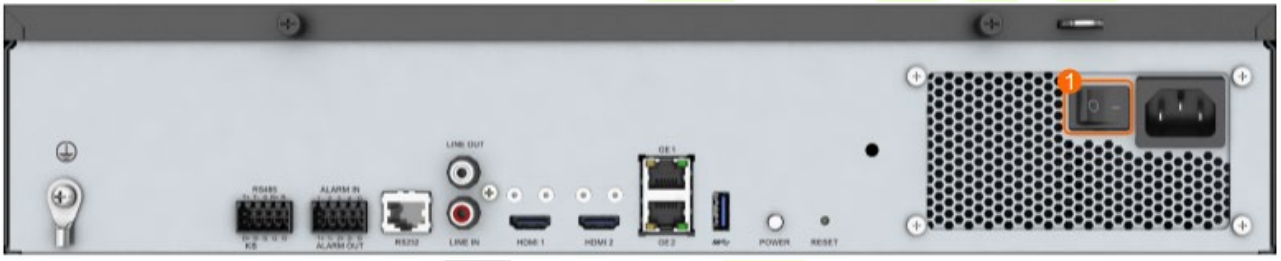
- An ESD bag and a PH2 Phillips screwdriver are available.
- A new hard disk is available.

Procedure

- **Install the new hard disk.**

The method of expanding non-RAID disks is similar to that of expanding RAID 5 disks. The following describes how to expand RAID 5 disks as an example.

1. Wear insulation gloves and connect the ground terminal of the ESD wrist strap into the ESD jack in the cabinet or on the workbench.
2. Power off the device, as shown in below.



3. Install the new hard disk.

   For details about how to install the new hard disk, see the Quick Start delivered with the product.
4. Power on the device.
5. Check whether the hard disk status indicator on the front panel is normal.
   - If the hard disk status indicator is green, the hard disks are normal.
   - If the hard disk status indicator is red, at least one hard disk is faulty.

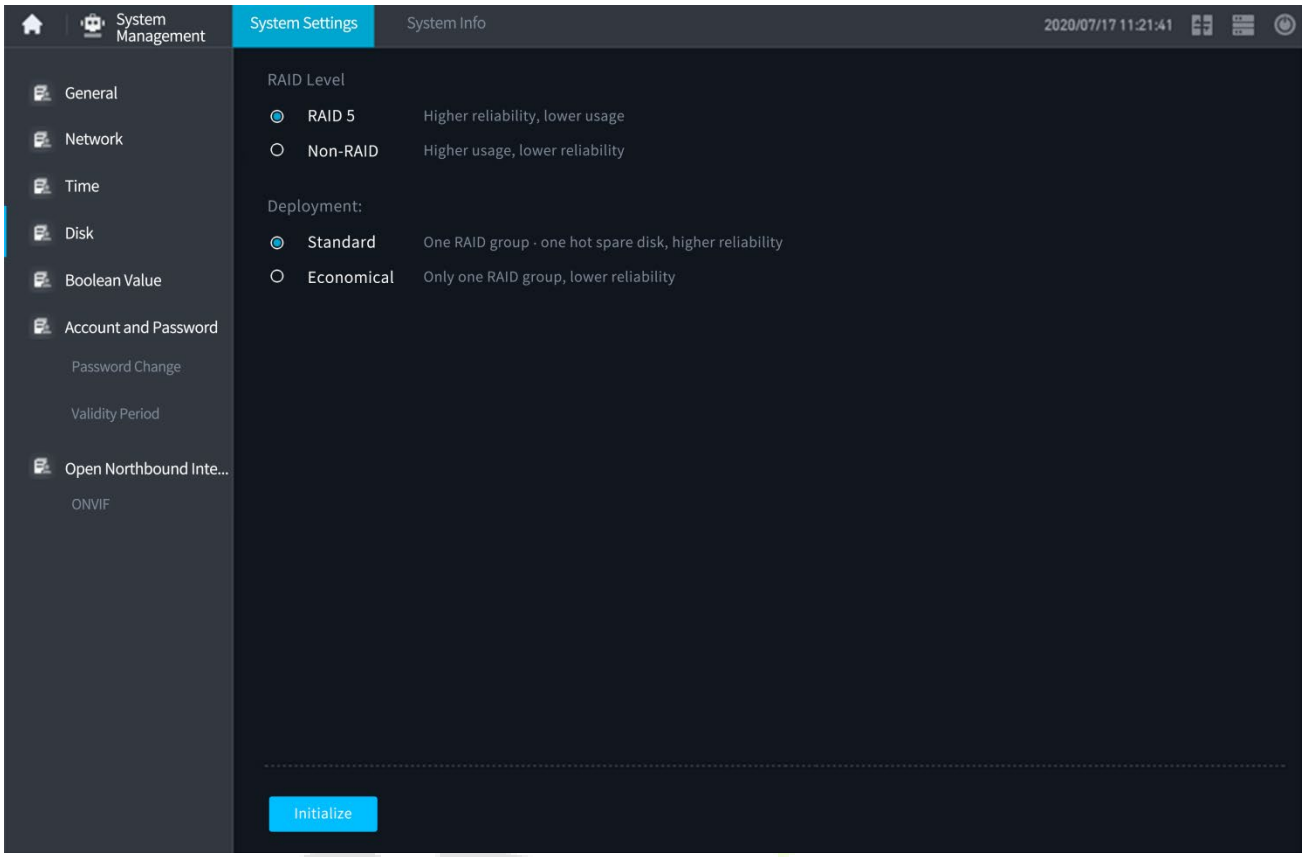
     If the new hard disk is abnormal, contact technical support.

- **LDU Scenario: Add a hard disk to the original RAID.**

1. Log in to the LDU as the admin user.
2. Right-click on the desktop to access the main menu.
3. Choose System Management > Disk Configuration.
4. It takes about 2 minutes for the LDU to read the hard disk status after the new hard disk is installed.
5. Add the new hard disk to the original RAID, as shown in below.

NOTE:

- In capacity expansion scenario, the system expands the hard disks based on the existing RAID type. The **RAID Mode and RAID Configuration Mode** parameters do not need to be set.



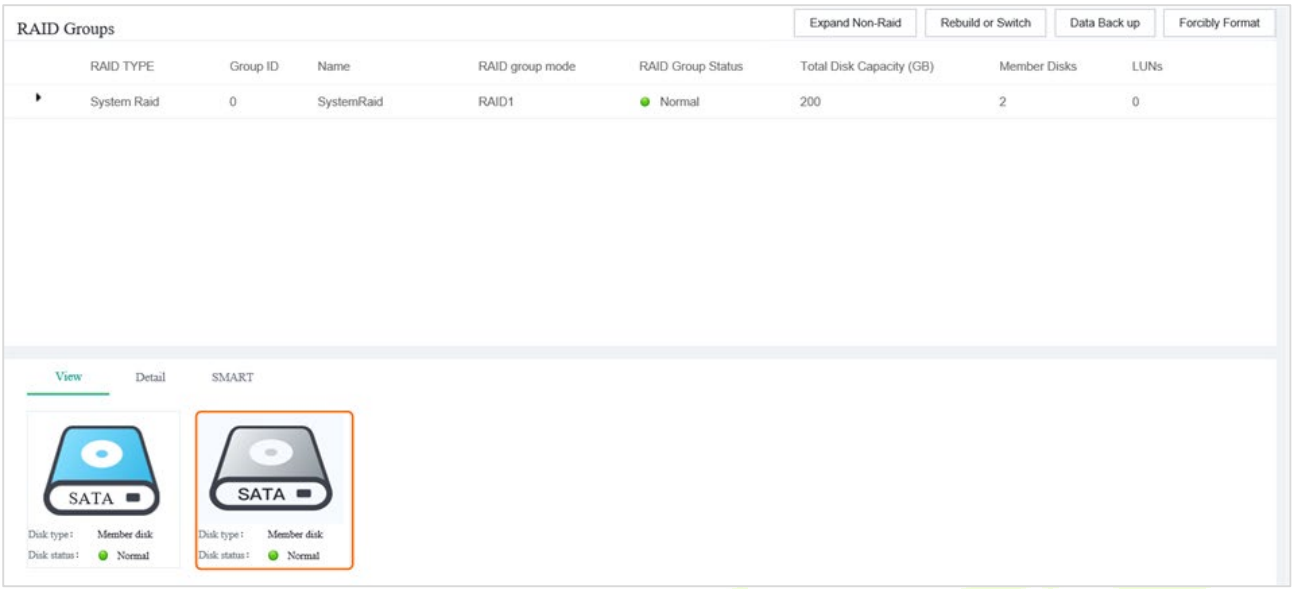
6. It takes about 5 to 10 minutes to expand the hard disks.

- **AS1700 Scenario: Add a hard disk to the original RAID.**

1. Log in to the AS1700 as the **admin** user.
2. Choose **Local Configuration > Local Disk > View**.

   It takes about two minutes to display the hard disk status on the AS1700 after the new hard disk is installed.

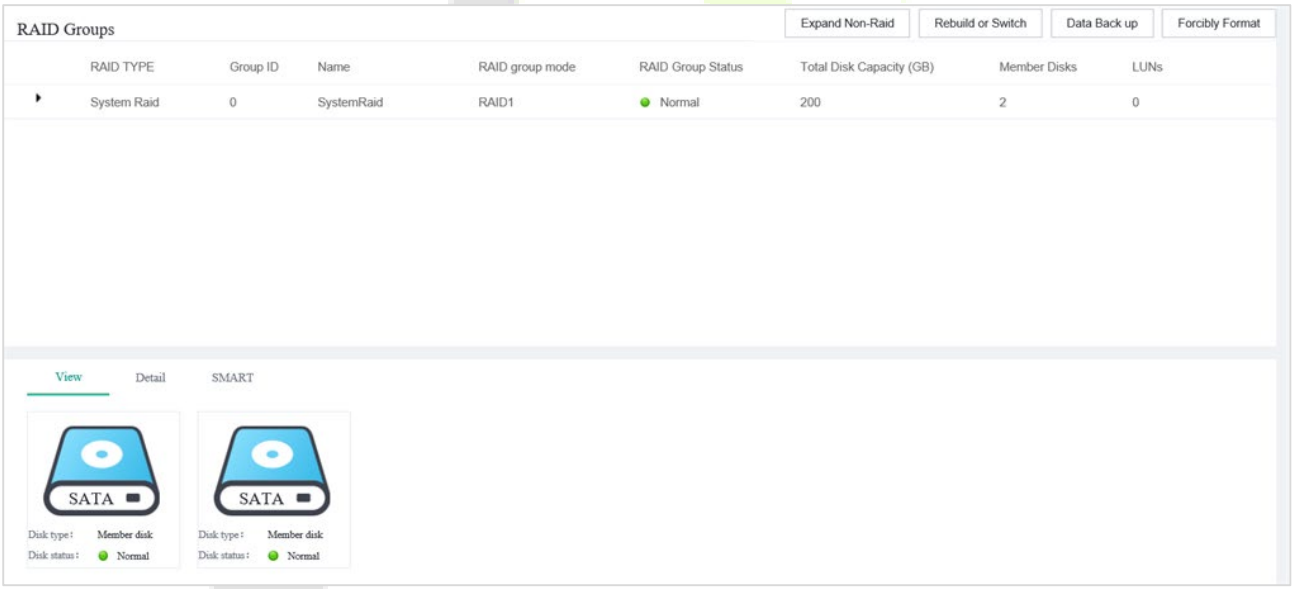
   The drive letter in gray shading is the new hard disk, as shown in below.



3. Click **Expand Non-Raid** to add the new hard disk to the original RAID.

   It takes about 5 to 10 minutes to expand the capacity of hard disks.

   After the capacity expansion is complete, the state of the new hard disk changes from **Idle disk** to **Member Disk**, as shown in below.



4.6.4.2 Switching the Disk Mode

CAUTION

Switching the disk mode may cause loss of all the recording data in the current disk. Exercise caution when performing this operation.

The following table describes the restrictions on the hard disk quantity when the disk mode is switched.

Restrictions Description

Current Disk Mode	Target Disk Mode	Hard Disk Quantity
Non-RAID mode	RAID 5 (economical configuration)	At least three hard disks
	RAID 5 (recommended configuration)	At least four hard disks
RAID 5 (economical configuration)	RAID 5 (recommended configuration)	At least four hard disks
	Non-RAID mode	N/A
RAID 5 (recommended configuration)	Non-RAID mode	N/A
	RAID 5 (economical configuration)	At least three hard disks

LDU Scenario

Step 1 Log in to the LDU as the **admin** user.

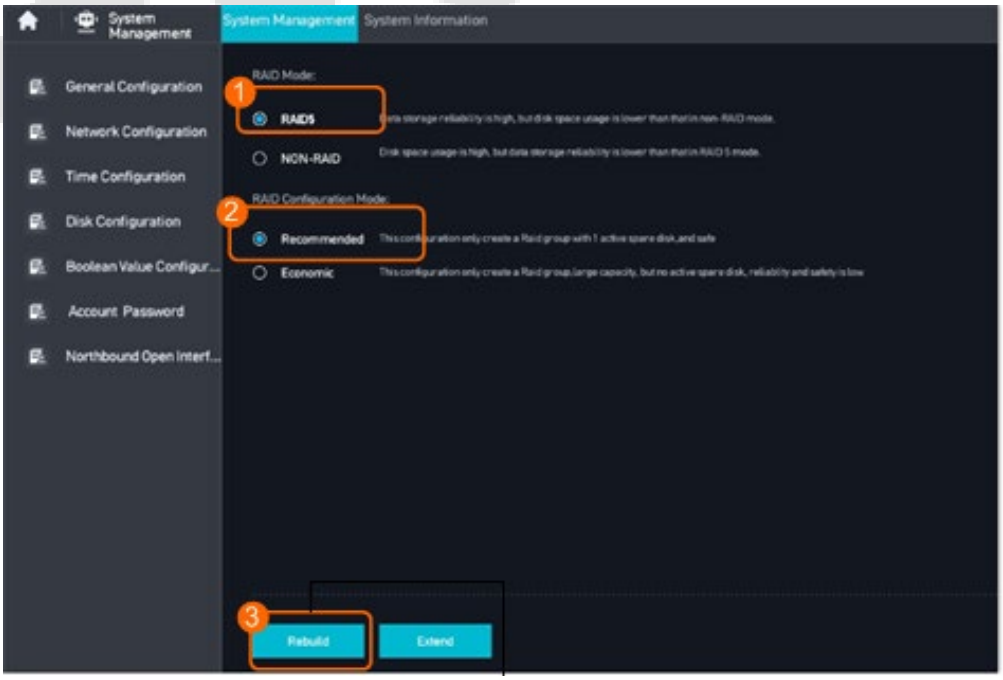
Step 2 Right-click on the desktop to access the main menu.

Step 3 Choose **System Management > Disk Configuration**.

Step 4 Switch the disk mode, as shown in below.

In this example, the RAID 5 mode is switched from **Economic** to **Recommended**.

It takes about 5 to 10 minutes to switch the disk mode.



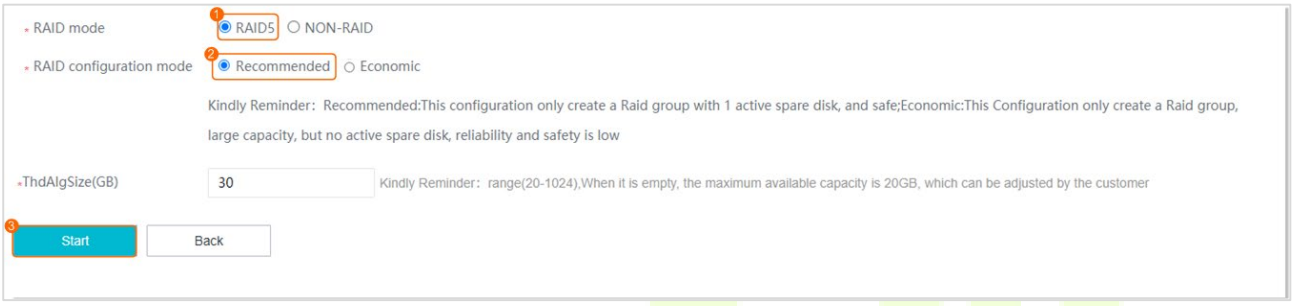
AS1700 Scenario

Step 1 Log in to the AS1700 as the **admin** user.

Step 2 Choose **Local Configuration > Local Disk > View** and click **Rebuild or Switch**.

Step 3 Switch the disk mode, as shown in below.

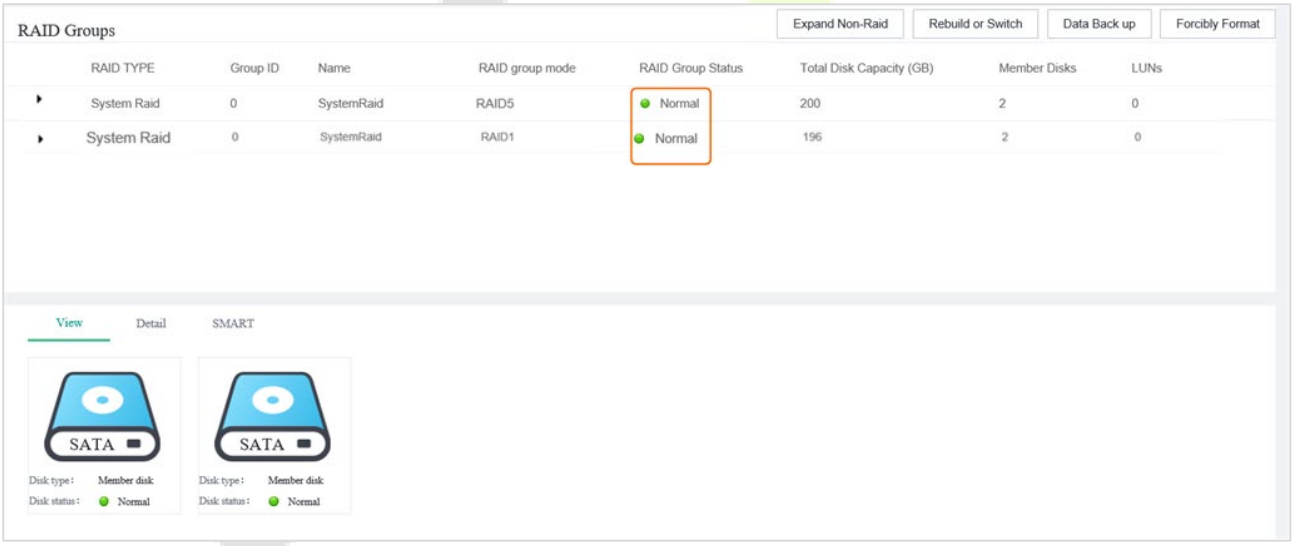
In this example, the RAID 5 mode is switched from **Economic** to **Recommended**.



Step 4 Enter the password of the current login user and click **OK** to verify the password.

It takes about 5 to 10 minutes to switch the disk mode.

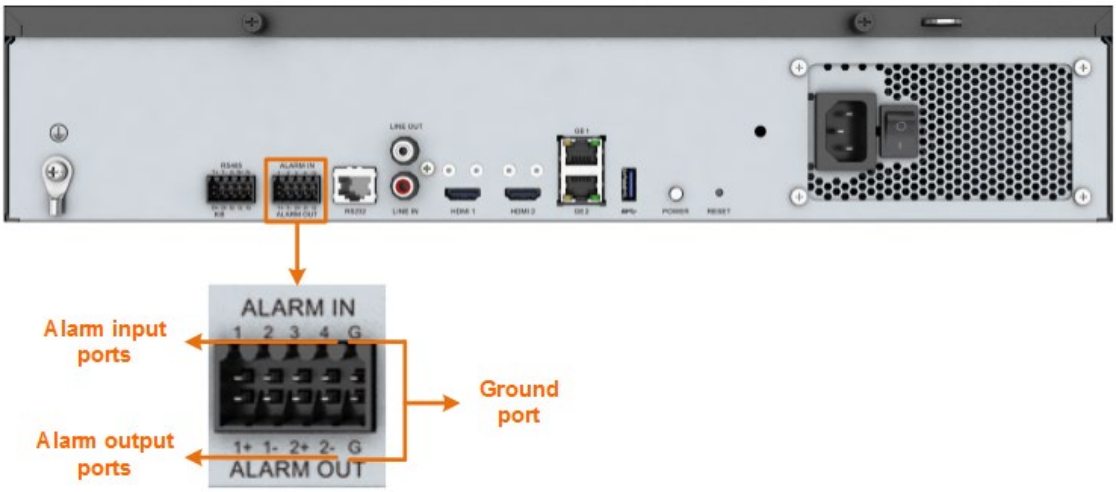
After the disk mode is switched, data RAID information and system RAID information are displayed in the RAID group list, as shown in below.



4.6.5 Boolean Value Settings

4.6.5.1 Connect to the Alarm Input and Output Ports

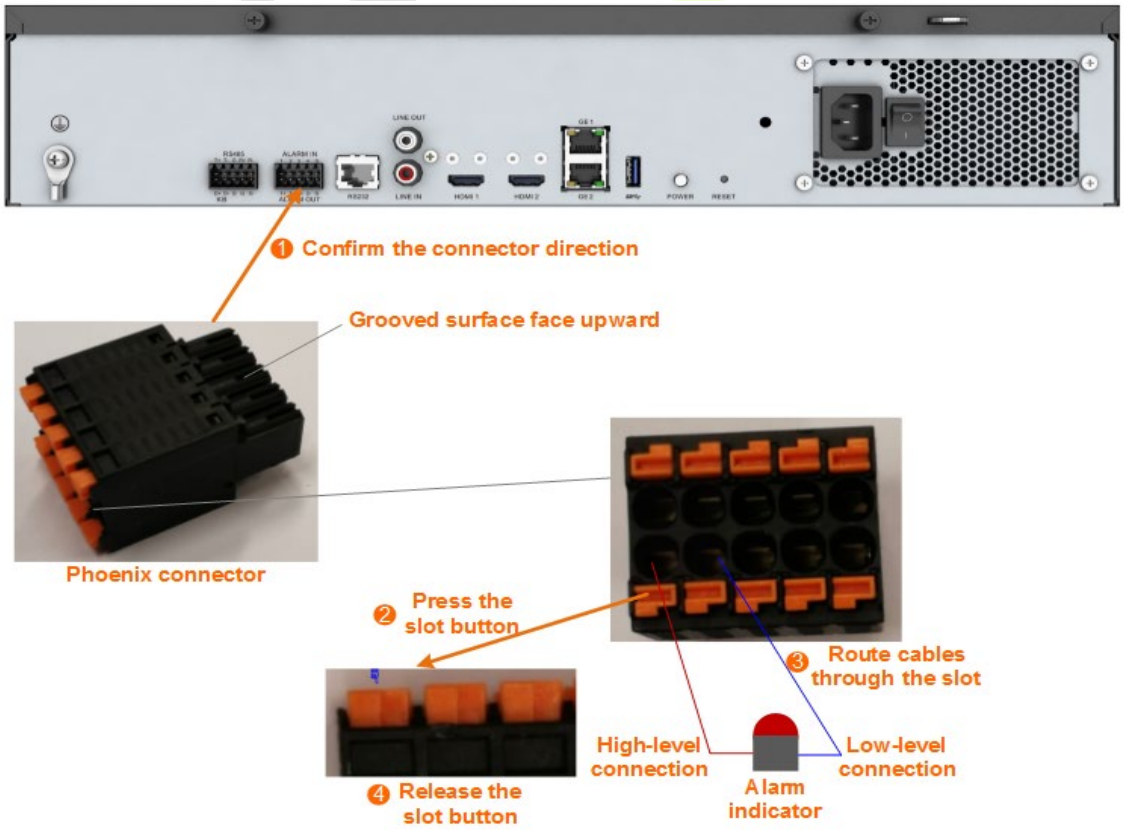
Port Description



- Ports 1, 2, 3, and 4 are alarm input ports, which can be connected to four alarm input devices.
- Ports 1+, 1-, 2+, and 2- are alarm output ports, which can be connected to two alarm output devices.

  Port 1+ is used for high-level output of line 1, and port 1- for low-level output of line 1. Port 2+ is used for high-level output of line 2, and port 2- for low-level output of line 2.
- Port G is the ground port, which is used with the alarm input and output ports. One ground port can be used to ground multiple alarm input and output ports at the same time.

Cabling Diagram



Procedure on the LDU

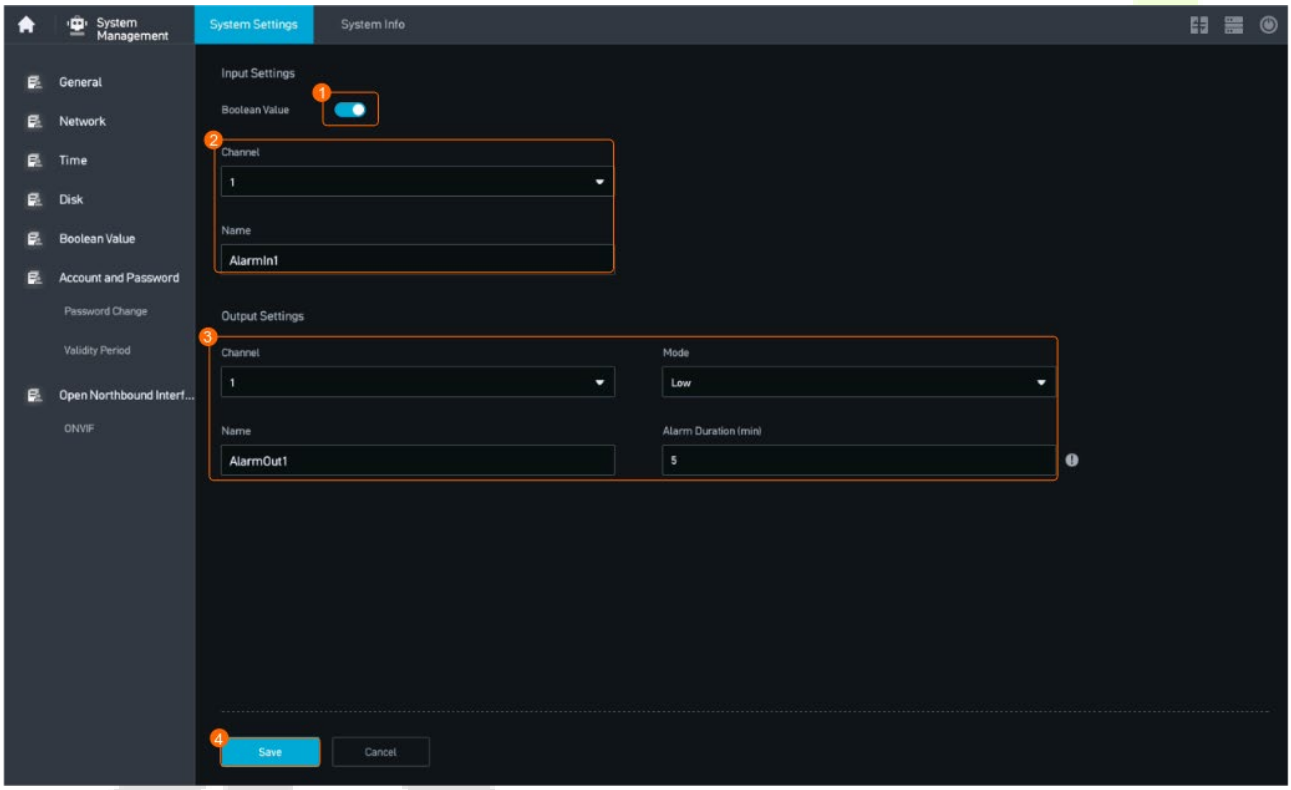
This section describes how to enable the Boolean value alarm output function in the AS1700.

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop to access the main menu.

Step 3 Choose **System Management** > **System Settings** > **Boolean Value**.

Step 4 Set Boolean value parameters, as shown in below



Parameter Description

Area	Parameter	Description
Input Settings	Channel	Select an alarm output channel based on the site requirements. The AS1700 supports only four alarm input devices.
	Name	Name of a Boolean value input channel.
Output Settings	Channel	Select an alarm output channel based on the site requirements. The AS1700 supports only two alarm output devices.
	Mode	Output mode of the level. • High • Low

Area	Parameter	Description
	Name	Name of a Boolean value output channel.
	Alarm Duration (min)	Boolean value output alarm duration. The alarm duration ranges from 1s to 3600s.

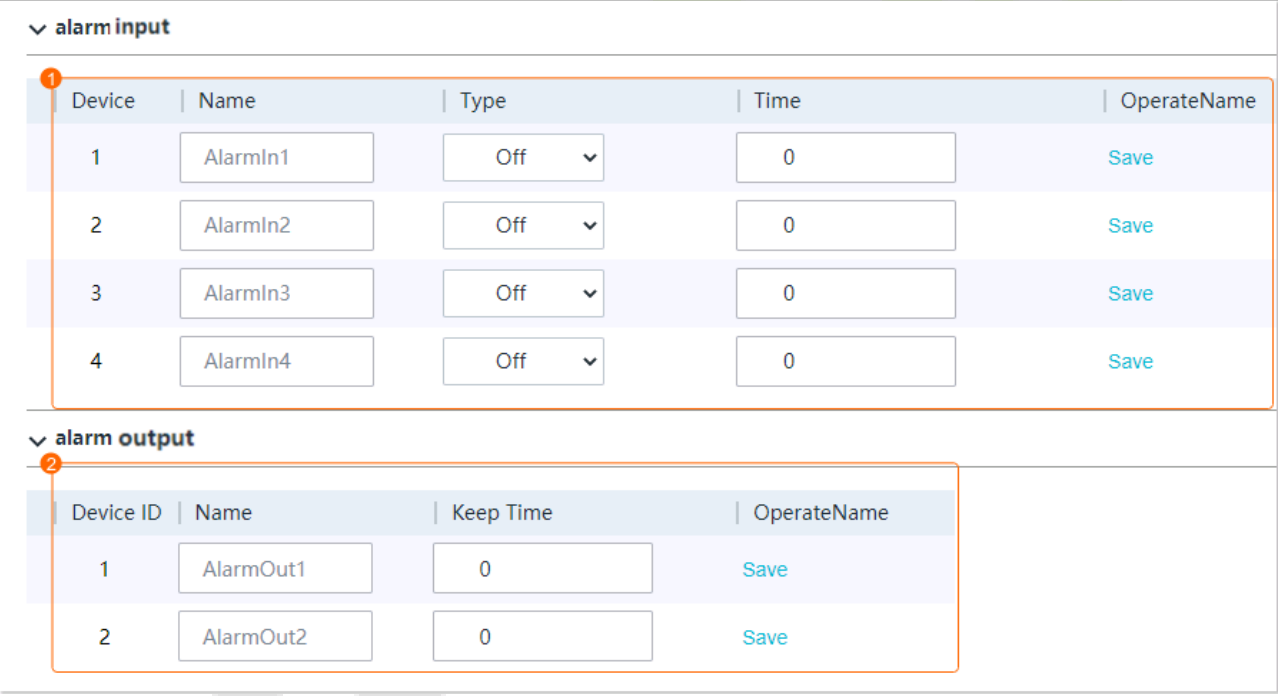
Procedure on the AS1700

This section describes how to enable the Boolean value alarm output function in the AS1700.

Step 1 Log in to the AS1700 as the **admin** user.

Step 2 Choose **SystemManagement** > **IO alarm**.

Step 3 Set Boolean value parameters, as shown in below.



Parameter Description

Area	Parameter	Description
alarm input	Name	Name of a Boolean value input channel. The AS1700 supports only four alarm input devices.
	Type	Select an alarm input mode. • Steady on If you select **Steady on**, alarm input is enabled by default. • Steady off

Area	Parameter	Description
		If you **Steady off**, alarm input is disabled by default and enabled when an alarm is generated. • Off If you select **Off**, alarm input is disabled.
	Time	Interval between two alarms.
alarm output	Name	Select an alarm output channel based on the site requirements. The AS1700 supports only two alarm output devices.
	Keep Time	Boolean value output alarm duration. The alarm duration ranges from 1s to 3600s.

4.6.6 Account and Password Settings

4.6.6.1 Export the GUID File and Reset the Password

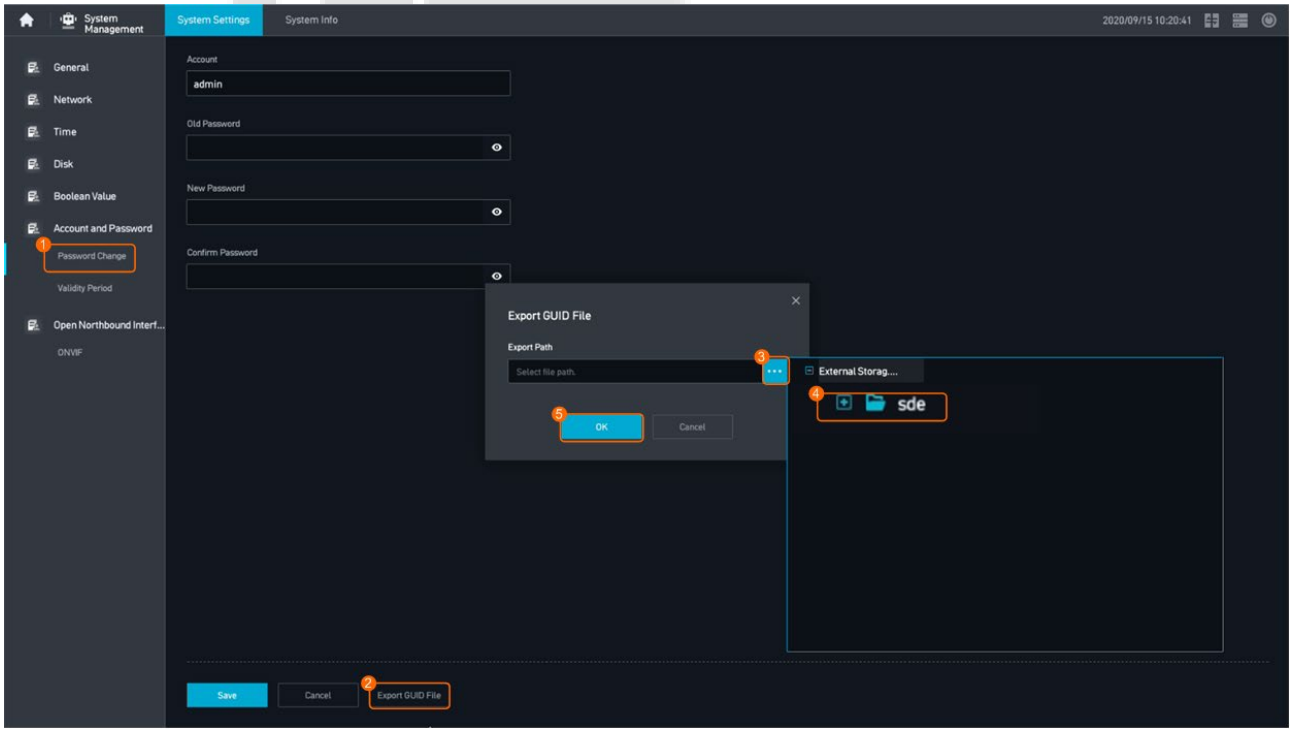
Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop to access the main menu.

Step 3 Choose **System Management** > **Account and Password** > **Password Change**.

Step 4 Export the encrypted GUID file to a removable disk, as shown in below.

A user who forgets the login password can import the encrypted GUID file to reset the password.



NOTE:

- After the encrypted file is exported, remove the removable disks (such as removable hard disks and USB flash drives) timely and keep them properly to prevent leakage of personal privacy data.

Step 5 On the LDU login page, click **Forget**, import the encrypted GUID file, and change the login password of the **admin** user.

4.6.6.2 Change the Password Validity Period

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop to access the main menu.

Step 3 Choose **System Management** > **Account Password** > **Password Validity Period**.

Step 4 Select **Enable Validity** and set **Password Validity Period**.

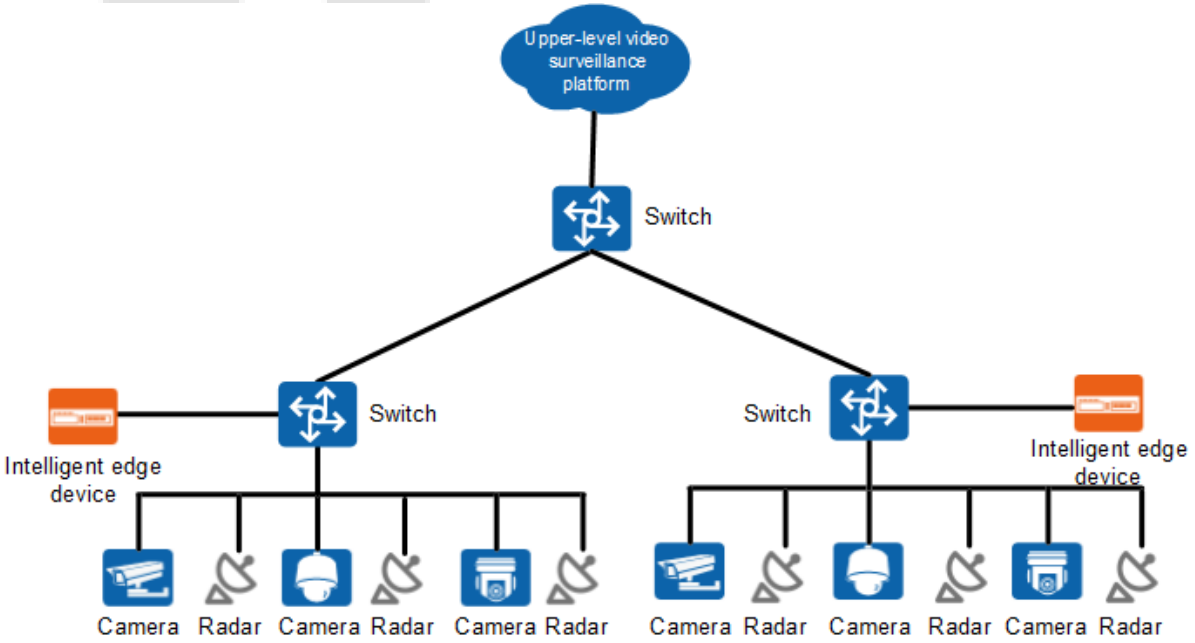
Deselect **Enable Validity** and you can set your password to be permanently valid.

4.6.7 Open Northbound Interface

4.6.7.1 Configuring the AS1700 for Connecting it to the Upper-Level Surveillance Platform as an NVR

Scenario Description

The AS1700 can be connected to the upper-level surveillance platform as an NVR, as shown in below.



ONVIF-based Access

1. Application Limitations

- After AS1700 is connected to the upper-level platform, you can perform live video viewing and PTZ control only on cameras under the AS1700.
- The upper-level platform needs to proactively obtain the camera status under AS1700. Currently, AS1700 cannot push the camera status.

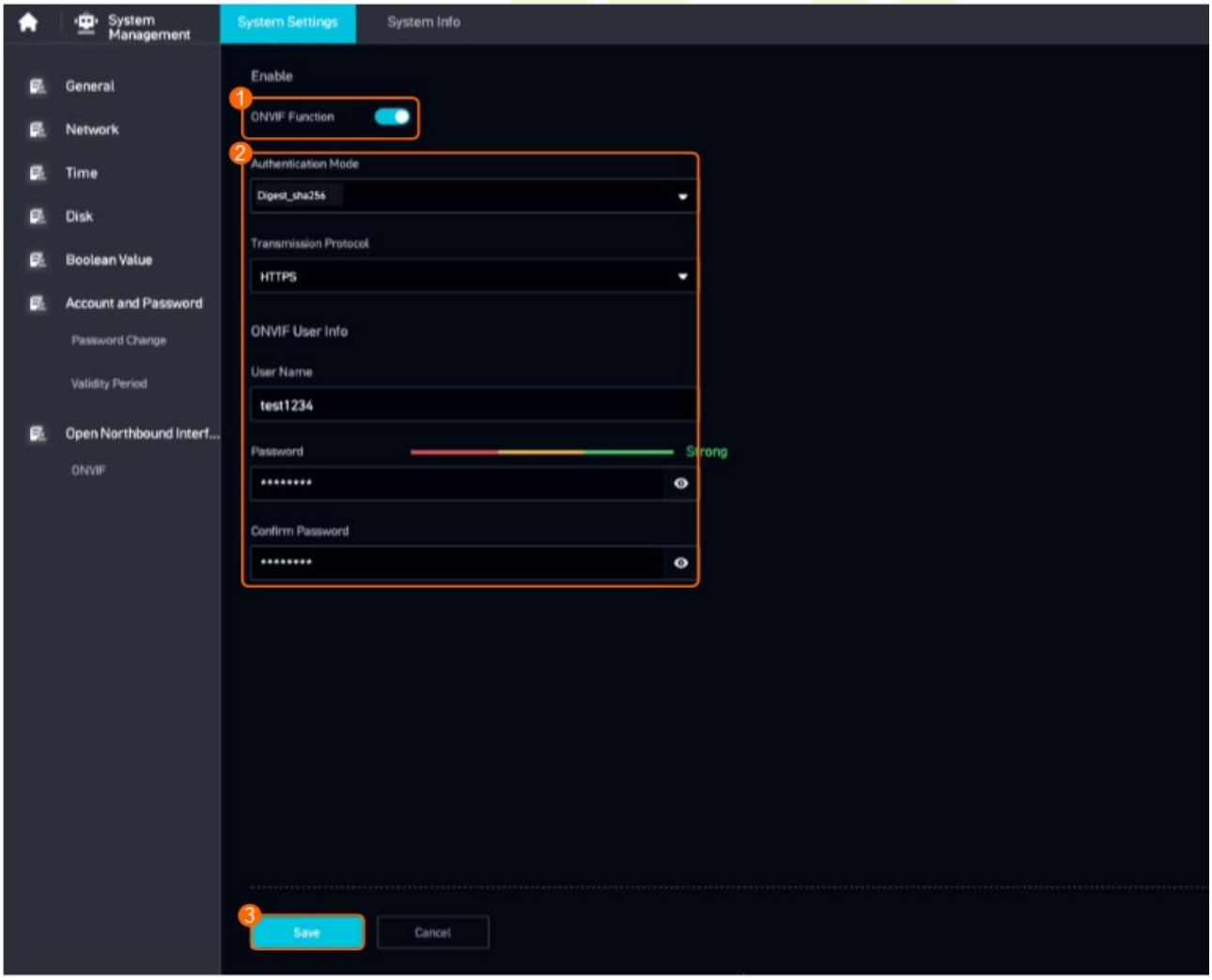
2. Configuring Data on the AS1700

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **System Management**.

Step 3 Choose **System Configuration** > **Open Northbound Interfaces** > **ONVIF**.

Step 4 Configure the ONVIF function, as shown in below.



Parameter Description

Parameter	Description
ONVIF Function	Enable this function.
Authentication Mode	ONVIF authentication mode. The default value is **Digest_sha256**. • Digest_sha256 • Digest_md5_and_sha256 • Digest • Digest/WSSE • WSSE • None: No authentication is performed, which poses security risks. Exercise caution when selecting this mode. **The WSSE authentication mode has security risks. If you select this mode, the system displays a message indicating that the system is prone to attacks. For security purposes, you are advised to enable authentication and use the Digest authentication mode.**
Transmission Protocol	Transmission protocol for connecting the device to the upper-level surveillance platform. The value must be the same as the transmission protocol configured for the upper-level surveillance platform. • HTTP • HTTPS • HTTP/HTTPS HTTP has security risks. If you select **HTTP**, the system displays a message indicating that the system is prone to attacks. Exercise caution when using this protocol.
User Name/Password	User name and password for connecting the device to the IVS3800 or IVS9000 through ONVIF. You are advised to create a complex password. For details about the password complexity requirements, see 5.7.5.3 Suggestions on Password Maintenance. If you need to change the authentication user name or password, reset them and save the settings.

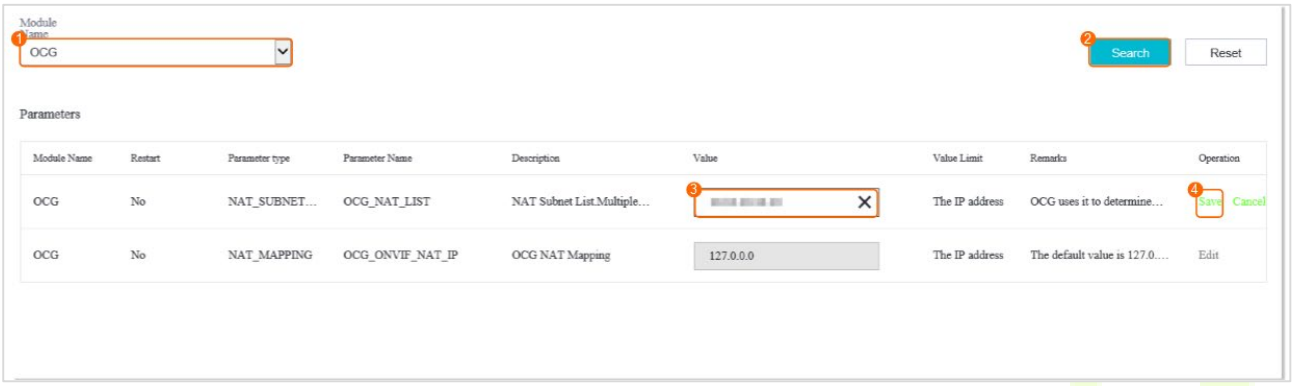
Step 5 (Optional) Set OCG parameters on the AS1700.

You do not need to set OCG parameters if the IP address of the upper-level surveillance platform is in the network segment 10.0.0.1 to 10.255.255.254, 172.16.0.1 to 172.31.255.254, or 192.168.0.1 to 192.168.255.254.

1. Log in to the AS1700 as the **admin** user.

2. Choose **Maintenance** > **Unified Configuration**.

3. Set OCG parameters, as shown in below.



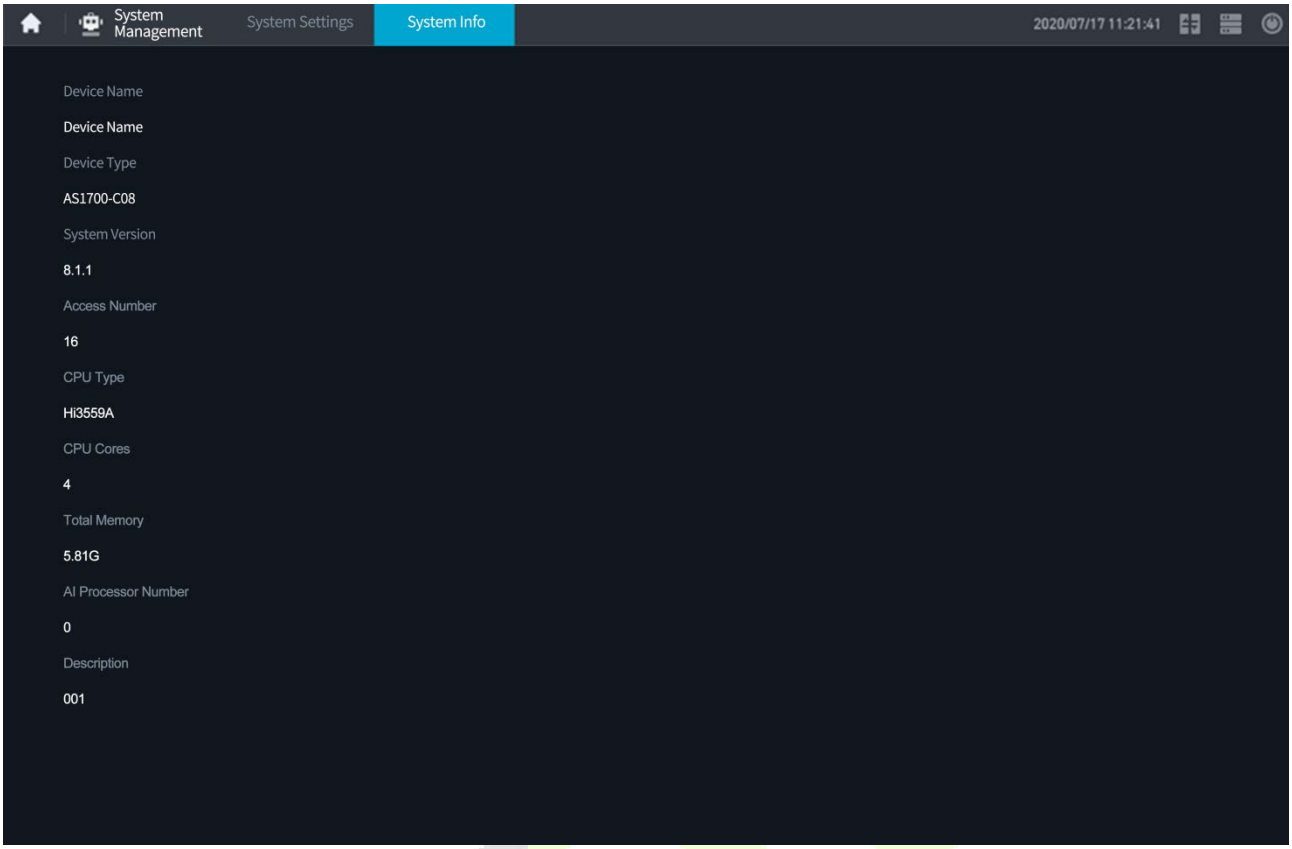
The following table describes the key parameters. You only need to set the parameters listed here.

Parameter Description

Parameter	Description
Value	IP address of the upper-level surveillance platform, which can be an IP address or network segment. • IP address: You can enter the IP address of the upper-level surveillance platform. If you enter multiple IP addresses, separate them with semicolons (;). • Network segment: If a large number of IP addresses need to be entered, you can use a network segment to specify the IP addresses. For example, if the IP addresses to be entered are *x.x.x.*20, *x.x.x.*21, *x.x.x.*22, and *x.x.x.*23, the value can be ***x.x.x.*0/24**. If you need to enter multiple network segments, separate them with semicolons (;). **NOTE:** Using a network segment brings security risks. You are advised to use IP addresses.

4.6.8 System Information

Through the system information option, you can view system information such as Device Name, Device Type, System Version, Access Number, CPU Type, CPU Cores, Total Memory, AI Processor Number, and Description.



4.7 Recording Management

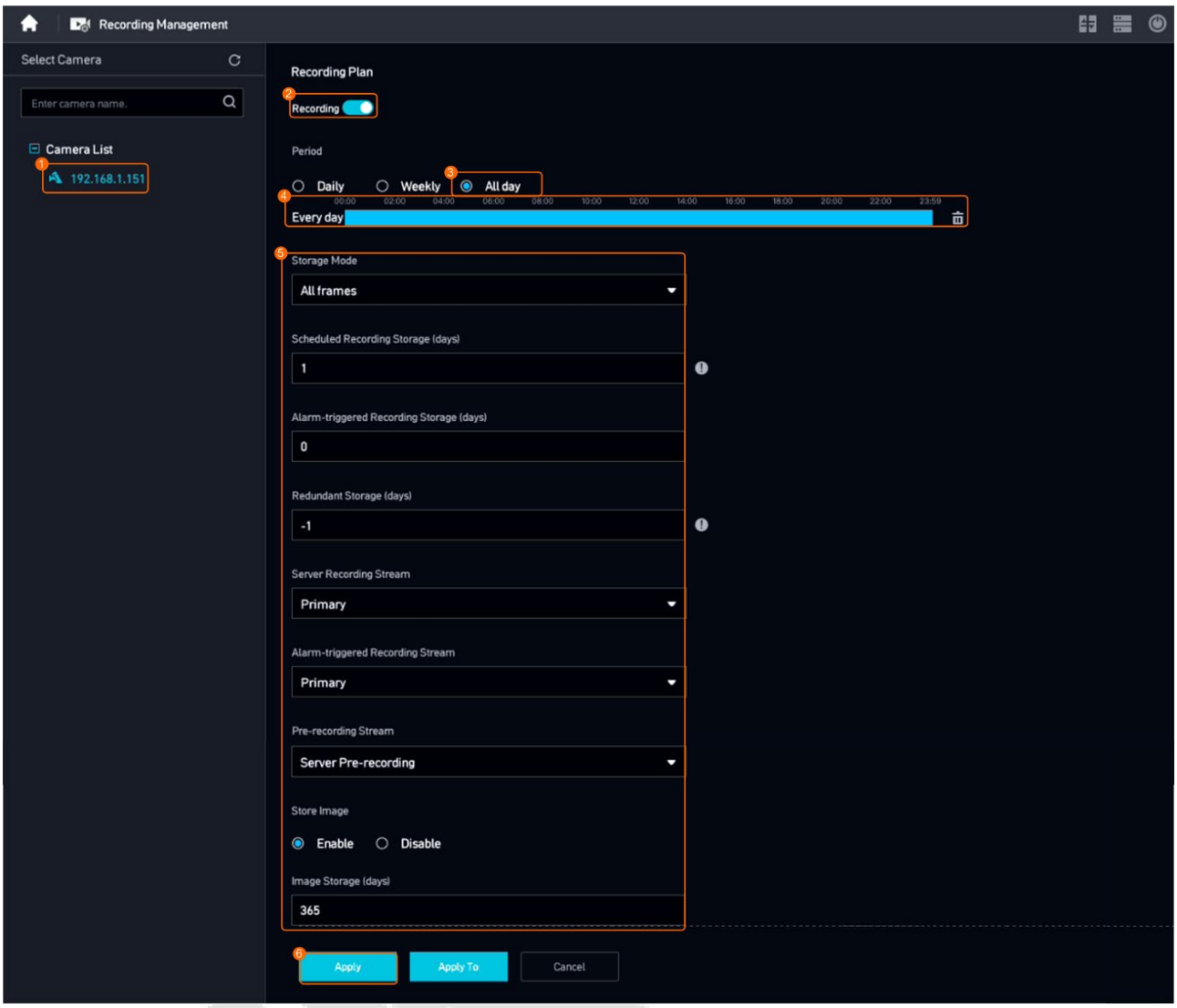
4.7.1 Setting Recording Parameters

For personal privacy reasons, the recording function is disabled by default. To use the recording function, enable the recording function and set a recording plan by referring to this section.

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **Recording**.

Step 3 Set recording management parameters and recording plans, as shown in below.



Key Parameter Description

Parameter	Setting
Recording Plan	Enable video recording.
Period	Period for recording video. A camera records video only in the specified period.
Storage Mode	Storage mode. Select **All frames** in this example. **All frames**: Recordings are stored completely within a specified period. After the period expires, the system gradually deletes the earliest recordings.
Scheduled Recording Storage (days)	Period for storing all frames of recordings, in days. The default value is **0**, indicating that recordings are stored permanently.
Alarm-triggered Recording Storage (days)	Period for storing alarms, in days. The default value is **0**, indicating that recordings are stored permanently.

Parameter	Setting
Redundant Storage (days)	Set the redundant recording storage period as required. • **-1** (default value): By default, redundant recording storage is always provided for the camera. (Recordings are stored in RAID 5 mode.) • **0**: Redundant recording storage is not configured for the camera. Recordings are stored in non-RAID mode. • Other values: You are advised to set this parameter to a duration shorter than the complete storage duration or the duration for overwriting the earliest recordings upon insufficient space.
Server Recording Stream	Select a stream type for scheduled recording as required. • **Primary**: The primary stream of the camera is used. The primary stream features a high bit rate, definition, and bandwidth usage. • **Secondary stream**: Secondary streams of the camera are used. Secondary streams feature low bit rates, definition, and bandwidth usage. If the camera has multiple secondary streams, the parameter will display multiple secondary stream options such as secondary stream 1 and secondary stream 2. The system automatically selects a stream type based on the bandwidth and network quality.
Alarm-triggered Recording Stream	Stream type used for scheduled alarm-triggered recording when a camera generates an alarm.
Pre-recording Stream	When a camera generates an alarm, the system pre-records the video generated 10s before the alarm is generated. Only PU pre-recording is supported.
Store Image	Indicates whether to store the intelligent images captured during scheduled recording. Set this parameter as required. • Enable • Disable
Image Storage (days)	Set the period for storing captured intelligent images as required.

5 Login to the AS1700

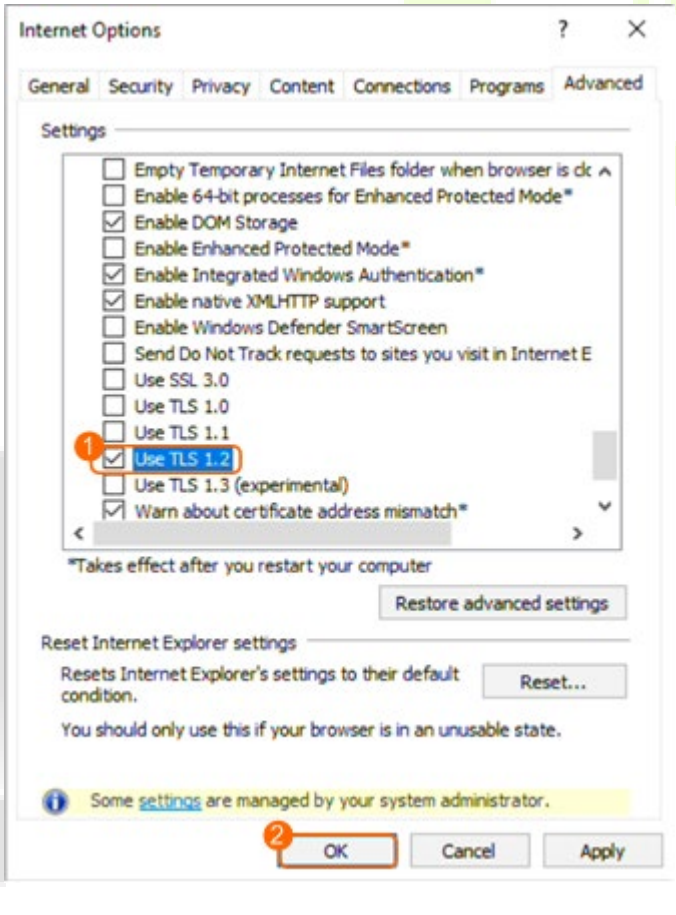
Application Limitations

- Browser: Internet Explorer 10.0 or later
- Operating system: 32-bit or 64-bit Windows 7/10

Procedure

Step 1 Open Internet Explorer and set browser parameters.

1. Choose **Settings** > **Internet Options** > **Advanced**.
2. Select **Use TLS1.2**, as shown in below.



Step 2 Enter **https://*IP address*:8443** in the address box, and press **Enter**.

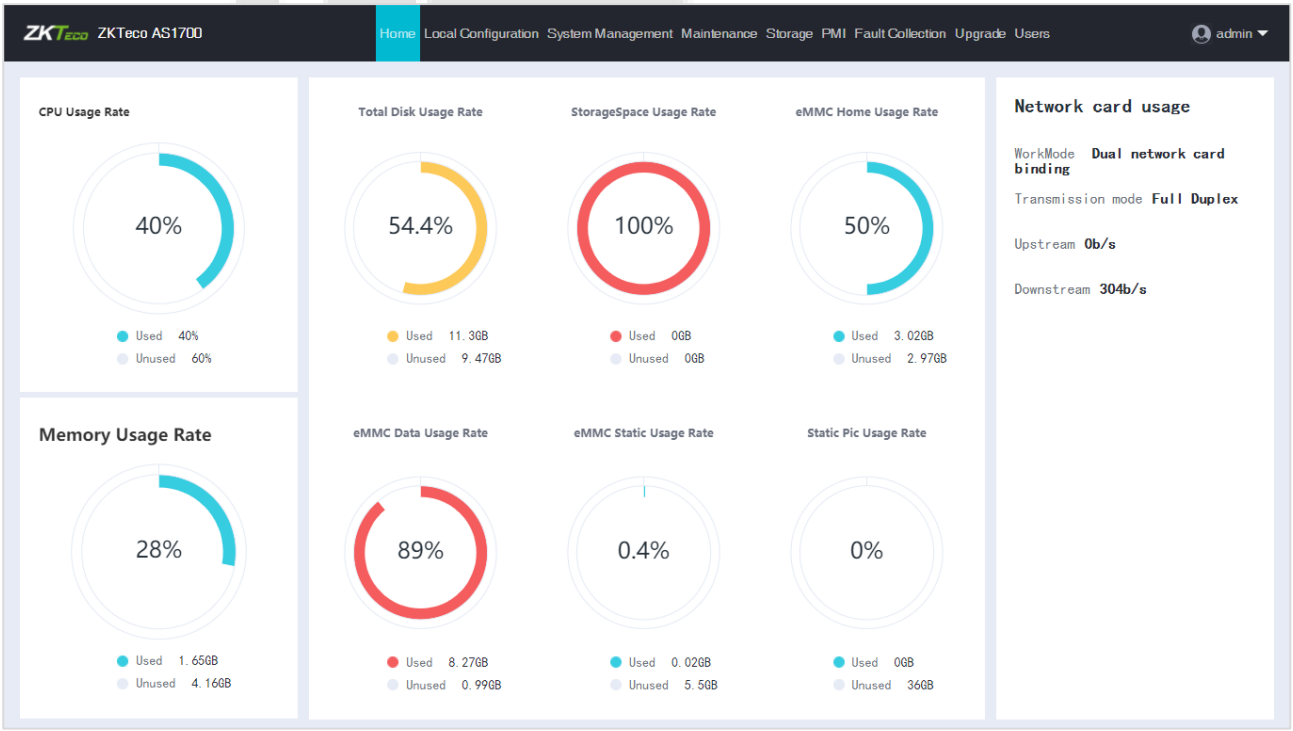
- In the preceding URL, *IP address* indicates the IP address of the AS1700.
- If dual network adapters are enabled for the AS1700, the IP address of the GE1 network port (northbound interconnection service) is 10.10.10.10, and the IP address of the GE2 network port (southbound interconnection service) is 192.168.3.11, you can enter

https://192.168.3.11:8443 or **https://10.10.10.10:8443** in the address box of a browser to log in to the AS1700.

Step 3 Set the service system and operating system passwords at the first login, For details, please refer to 3.2Configuring the Startup Wizard.

Step 4 After completing the password setting, enter the admin user name and password to log in to AS1700, as shown in below.

Step 5 The home page of successful login to AS1700 is shown in the figure below.



6 Login to the Camera Web System

Prerequisites

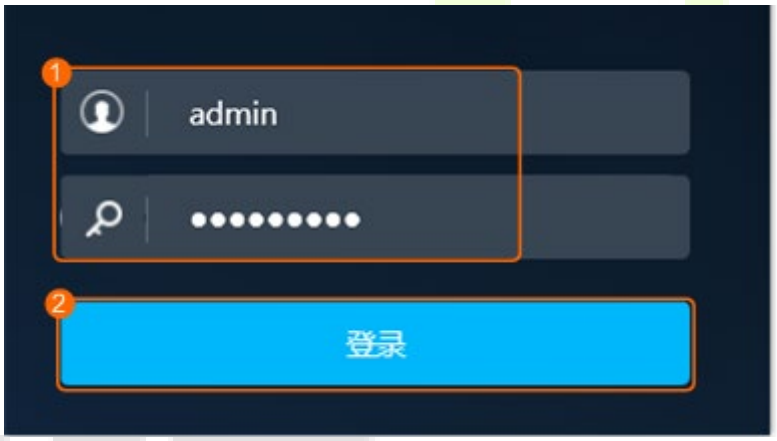
- Cameras have been powered on and connected to the network. For details, see related camera documents.

Procedure

Step 1 Enter **https://*camera IP address*** in the Internet Explorer address box, and press **Enter**.

Step 2 Set the password according to instructions during first login. For a non-first login, go to 3.

Step 3 Enter the password and click **Log In**.



NOTE:

- The login page varies depending on the camera model.

7 Others

7.1 Connecting Cameras

7.1.1 HWSDK-based Access

Context

- HWSDK-compliant cameras can be connected in any of the modes illustrated in table below.

Application Scenarios

Mode	Application Scenario	Remarks
Auto Discovery	The network cables of the device and cameras are connected to the network ports corresponding to **the same VLAN** as the switch.	You can use the default IP addresses of the cameras without manual configuration.
By Network Segment	The device can be connected to the **network where the IP addresses of the cameras are located**. The network cables can be connected to the network ports corresponding to the same VLAN or different VLANs.	You need to log in to the camera web system to configure camera IP addresses.
One by One		

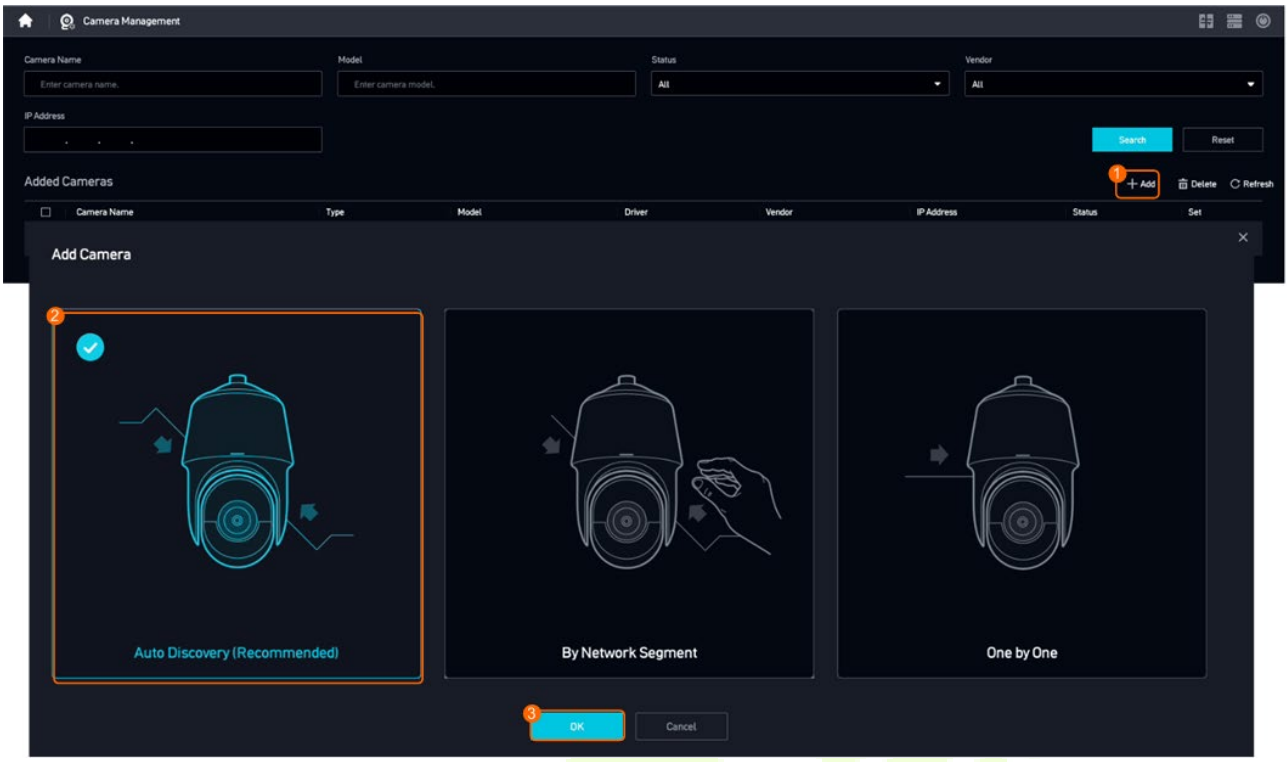
7.1.1.1 Auto Discovery

Step 1 Log in to the LDU as the **admin** user.

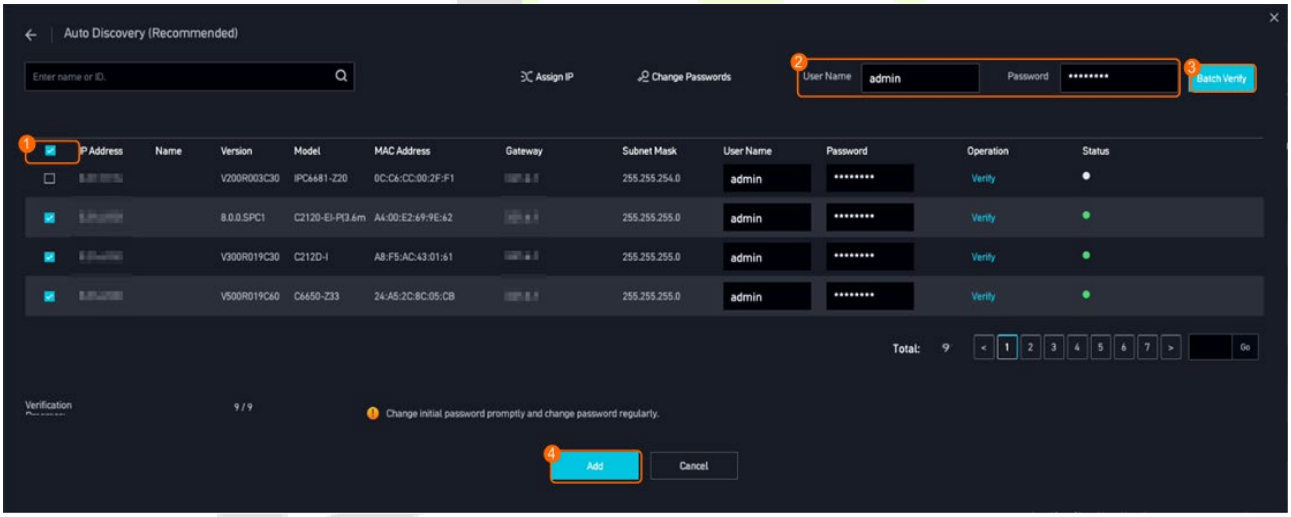
Step 2 Right-click on the desktop and choose **Camera Management**.

Step 3 Click **Add** and select **Auto Discovery (Recommended)**, as shown in below.

The device automatically searches for cameras that are on the same VLAN.



Step 4 Connect the cameras, as shown in below.



Parameter/Button Description

Parameter/Button	Description	Remarks
Batch Assign IP Addresses	The device assigns IP addresses to cameras in a unified manner. During the setting, you need to enter the password for registering a camera through the HWSDK protocol. The user name is fixed to **admin**.	-

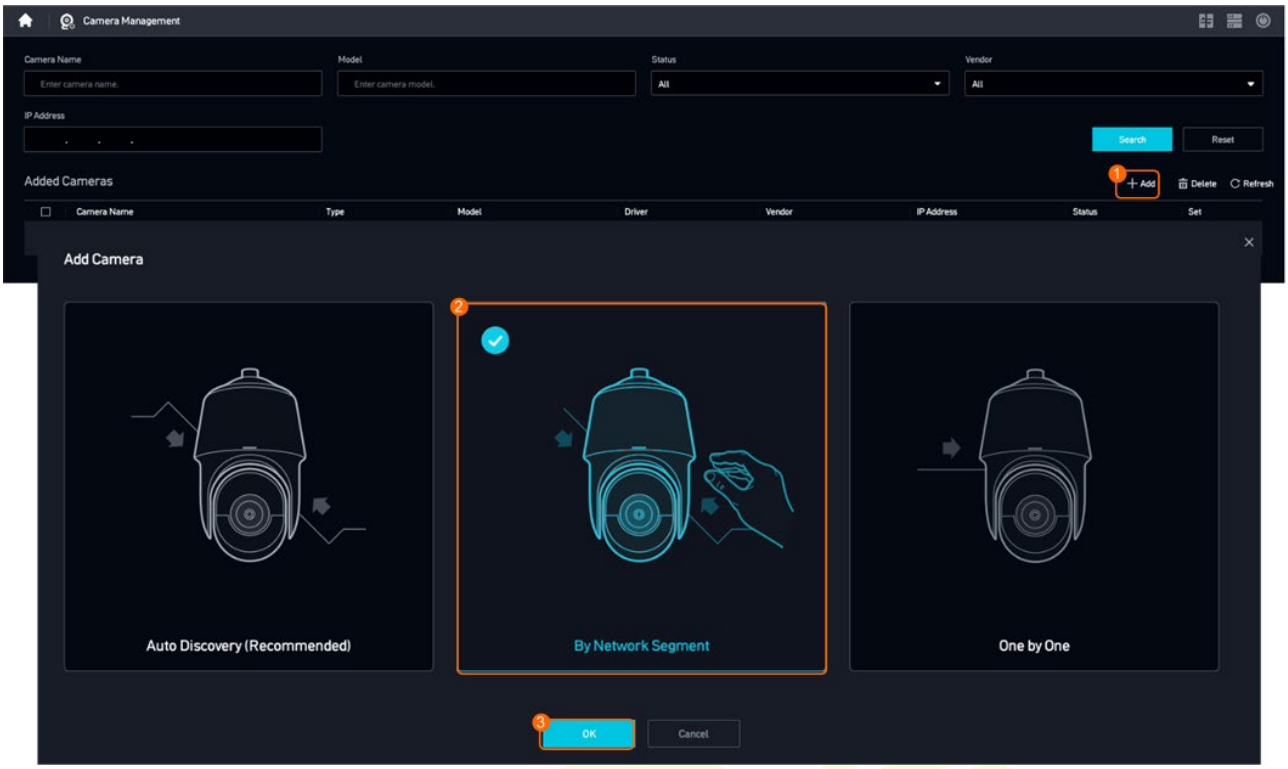
Parameter/Button	Description	Remarks
	NOTE: If an IP address in the assigned network segment has been occupied by another device, the camera may be assigned the same IP address as the device. As a result, the camera goes offline unexpectedly. Therefore, ensure that no IP address in the assigned network segment is in use.	
Change Passwords	Button for changing camera passwords in centralized mode on the device.	-
User Name/Password	User name and password for registering a camera through the HWSDK protocol.	-
Batch Verify	Button for verifying the registration user names and passwords of cameras in batches.	If the verification is passed,  is displayed. If not,  is displayed. If the user name or password of a camera has been changed after registration, the camera may fail the batch verification. You can configure the user name or password for the camera and then independently verify the camera.
Verify	Button for verifying the registration user name and password of a single camera.	

7.1.1.2 By Network Segment

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **Camera Management**.

Step 3 Click **Add** and select **By Network Segment**, as shown in below.

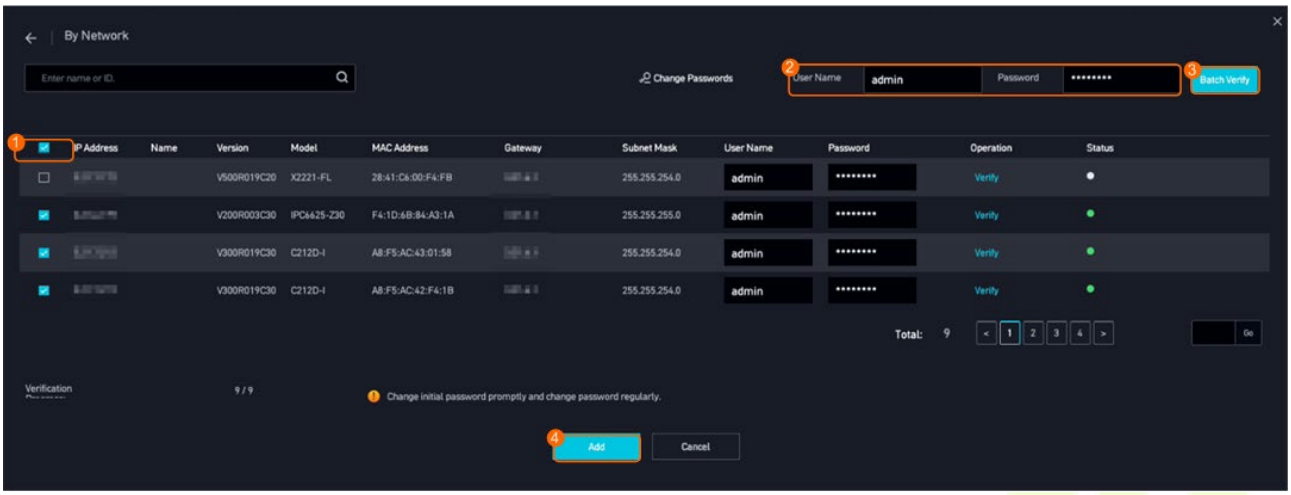


Step 4 Search for cameras, as shown in below.

Parameter Description

Parameter	Setting
Protocol	Select **HWSDK**.
Network Segment	Start and end IP addresses of the cameras. A precise network segment will shorten the search time.

Step 5 Verify cameras, as shown in below.



Parameter Description

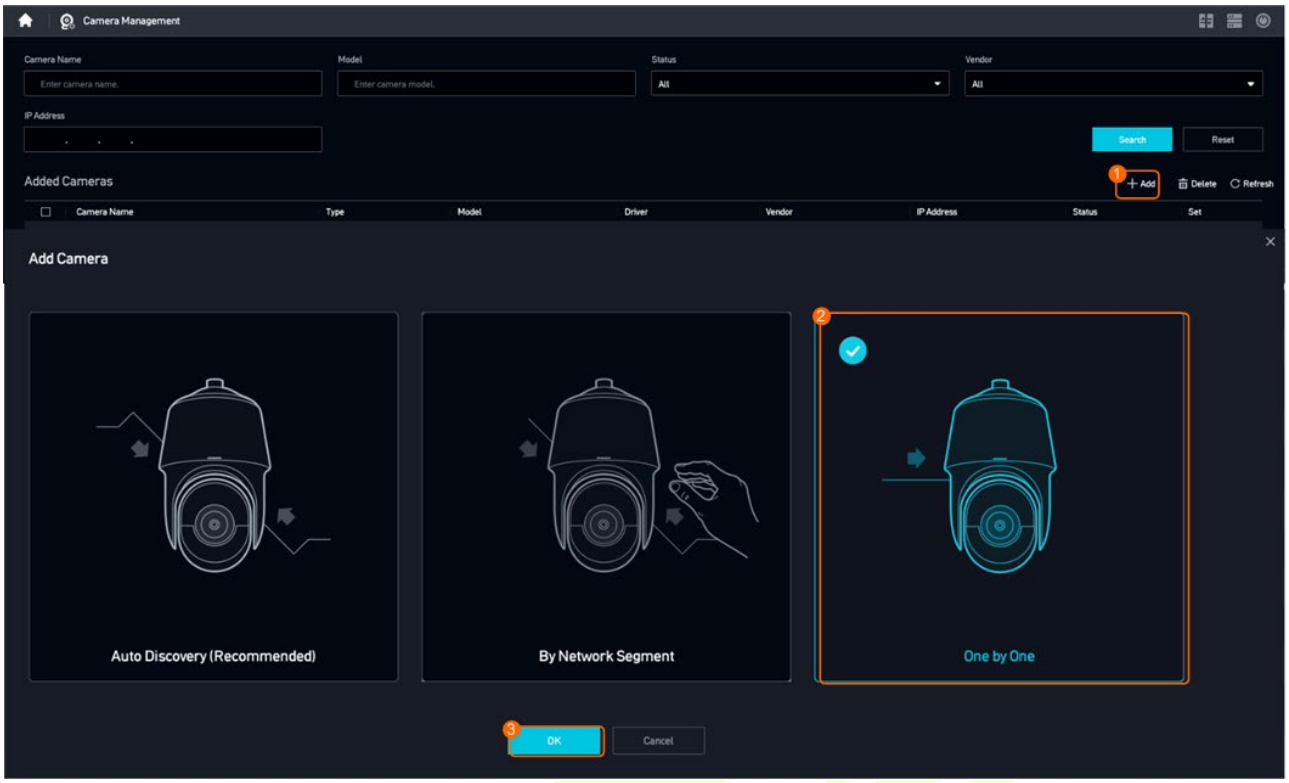
Parameter	Description	Remarks
Change Passwords	Button for changing camera passwords in centralized mode on the AS1700.	-
User Name/Password	User name and password for registering a camera through the HWSDK protocol.	-
Batch Verify	Button for verifying the registration user names and passwords of cameras in batches.	If the verification is passed, is displayed. If not, is displayed. If the user name or password of a camera has been changed after registration, the camera may fail the batch verification. You can configure the user name or password for the camera and then independently verify the camera.
Verify	Button for verifying the registration user name and password of a single camera.	

7.1.1.3 One by One

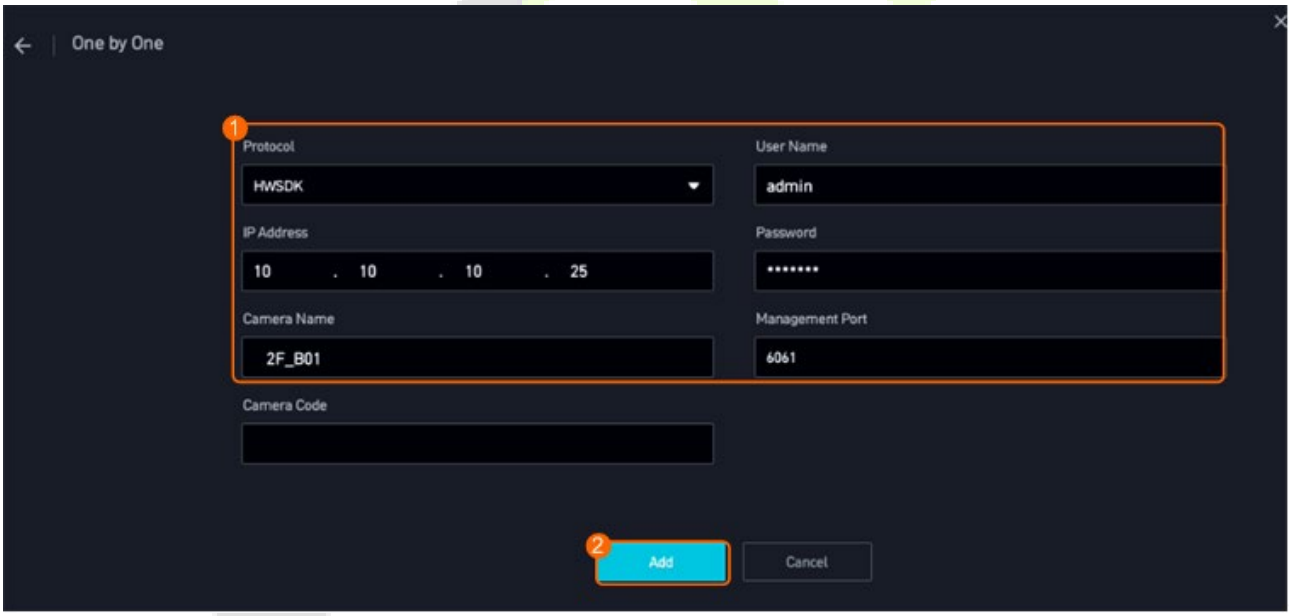
Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop and choose **Camera Management**.

Step 3 Click **Add** and select **One by One**, as shown in below.



Step 4 Add one camera, as shown in below.



Note: The following table describes the parameters. You only need to set the parameters listed here.

Parameter Description

Parameter	Description
Protocol	Select **HWSDK**.
IP Address	Camera IP address. Set it based on the site requirements.

Parameter	Description
Camera Name	Camera name. Customize the name.
User Name/Password	User name and password for registering a camera through the HWSDK protocol.
Management Port	• If the cameras use TLS for data transmission, set the port number to **6061**. • If the cameras use a non-encryption transmission protocol, set the port number to **6060**. Data transmission through non-encryption protocols may bring security risks. You are advised to use a cryptographic protocol.

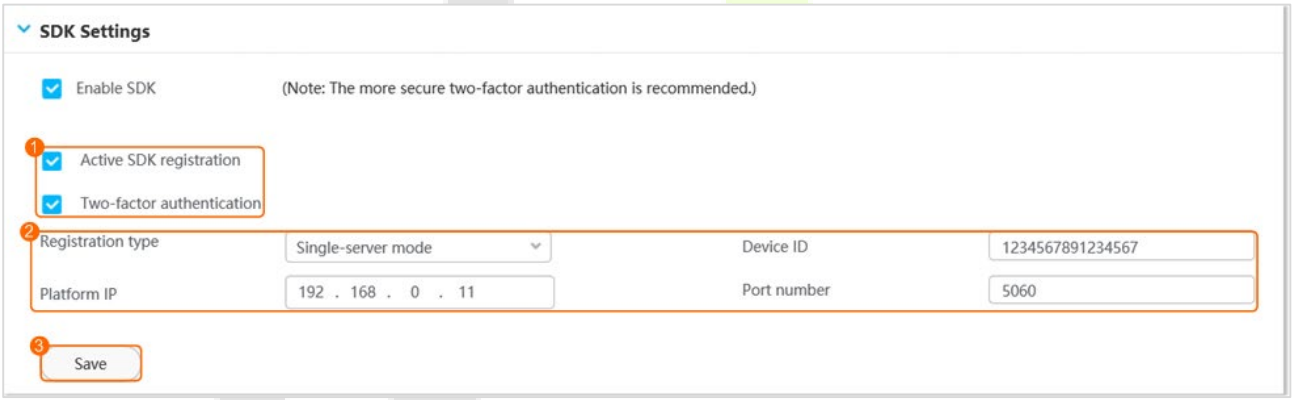
7.1.1.4 Active Registration

Step 1 Enable the proactive registration function on the camera.

a. Log in to the camera web system as the **admin** user.

b. Choose **Settings** > **Network** > **Platform Connection** > **SDK Settings**.

c. Enable the protocol, as shown in below.



Parameter Description

Parameter	Description
Active SDK registration	Indicates whether to proactively register a camera. If you select this check box, the camera will proactively be registered with the AS1700 using the HWSDK protocol.
Two-factor authentication	Authentication mode between the camera and the platform. If **Two-factor authentication** is selected, TLS authentication is used. If **Two-factor authentication** is not selected, password authentication is used. You are advised to select this check box to improve system security.
Registration type	Registration type. Select **Single-server mode**.

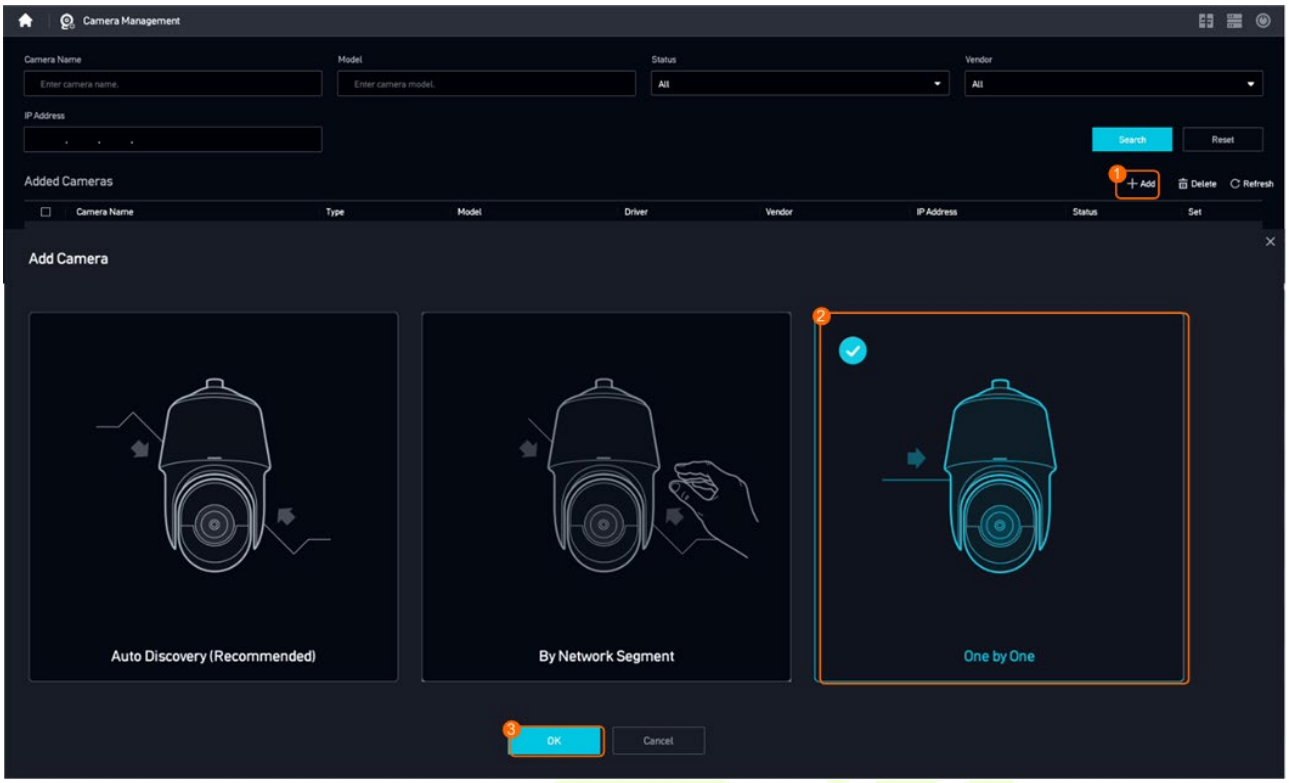
Parameter	Description
Device ID	Enter a 20-digit decimal number for connecting to the AS1700. • If the camera supports only 16-digit numbers, set this parameter to a 16-digit number. • If the camera supports numbers of 20 or more digits, set this parameter to a 20-digit number.
Platform IP	IP address of the AS1700.
Port number	• If **Two-factor authentication** is selected, the camera uses TLS. Set the port number to **5062**. • If **Two-factor authentication** is not selected, the camera does not use TLS. Set the port number to **5060**. To ensure system security, you are advised to use TLS. If a camera fails to be connected, rectify the fault by referring to 8.3 Failure to Verify a Camera When You Follow the Wizard to Add It.
Enable SDK	Select this check box when the camera is passively registered with the device through the HWSDK protocol. You do not need to set all the preceding parameters.

Step 2 Add cameras on the AS1700.

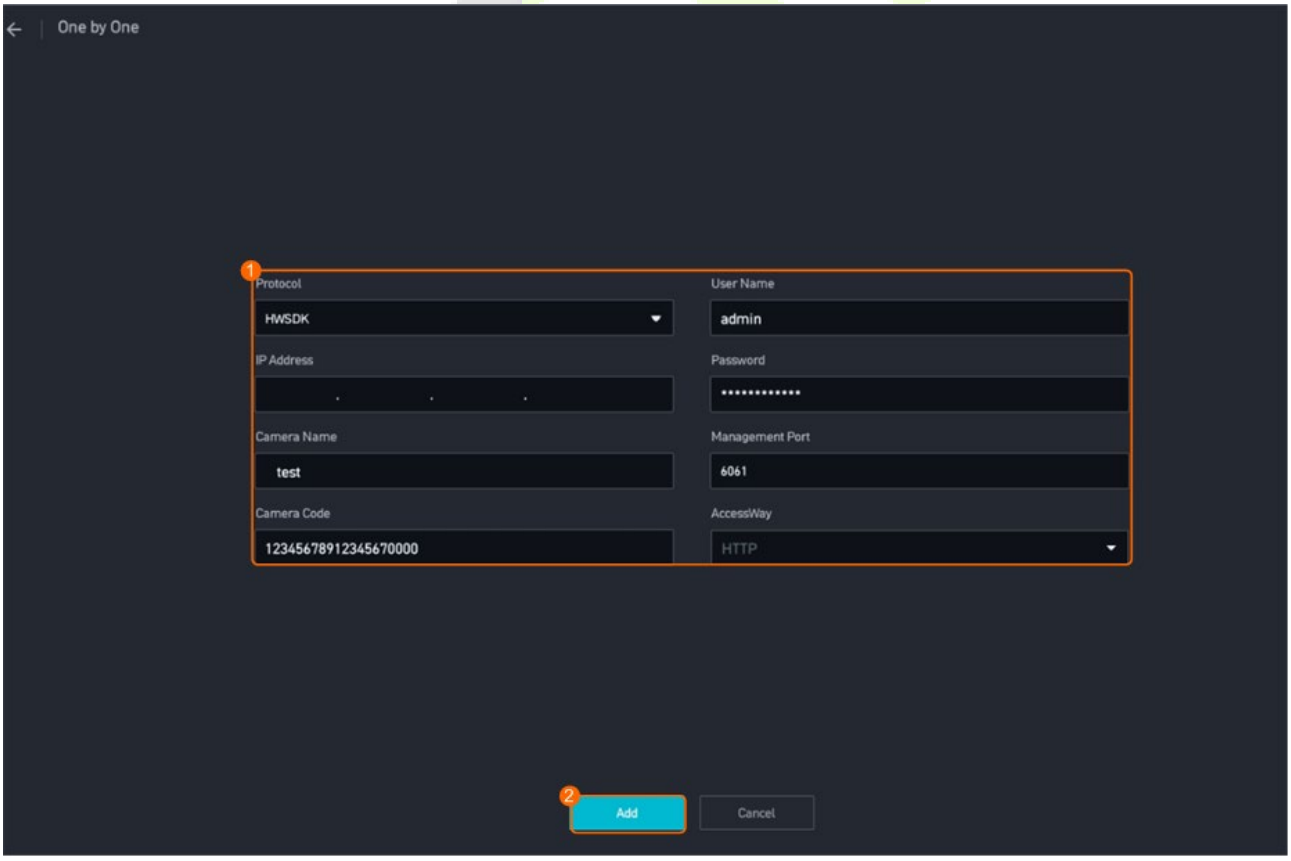
a. Log in to the LDU as the **admin** user.

b. Right-click on the desktop and choose **Camera Management**.

c. Click **Add** and select **One by One**, as shown in below.



Step 3 Add cameras one by one, as shown in below.



Parameter Description

Parameter	Setting
Protocol	Select **HWSDK**.
IP Address	You do not need to set this parameter.
Camera Name	User-defined camera name.
User Name/Password	User name and password for registering a camera through the HWSDK protocol.
Management Port	• If the cameras use TLS for data transmission, set the port number to **5062**. • If the cameras use a non-encryption transmission protocol, set the port number to **5060**. Data transmission through non-encryption transmission protocols may bring security risks. You are advised to use a cryptographic protocol. If a camera fails to be connected, rectify the fault by referring to 8.3 Failure to Verify a Camera When You Follow the Wizard to Add It.
Camera Code	The value must be the same as the device ID in **Step1**.

7.1.2 ONVIF-based Access

Context

- ONVIF-compliant cameras can be connected to the AS1700 in either of the modes illustrated in table below.

Application Scenarios

Mode	Application Scenario	Remarks
By Network Segment	The device can be connected to the **network where the IP addresses of the cameras are located**. The network cables can be connected to the network ports corresponding to the same VLAN or different VLANs.	You need to log in to the camera web system to configure camera IP addresses.
One by One		

7.1.2.1 By Network Segment

Step 1 Enable the ONVIF protocol on the camera side.

a. Log in to the camera web system as the **admin** user.

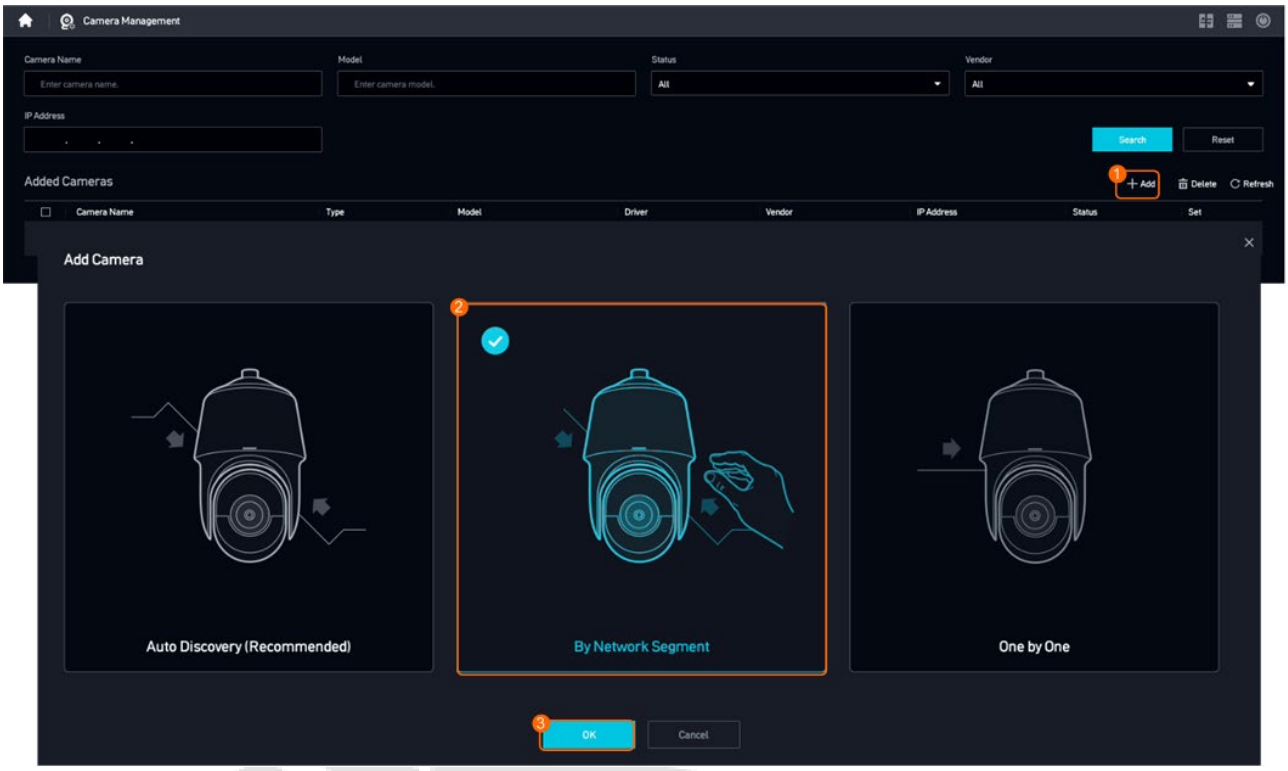
b. Choose **Settings** > **Network** > **Platform Connection** > **Second Protocol Parameters**.

c. Select **Enable ONVIF**.

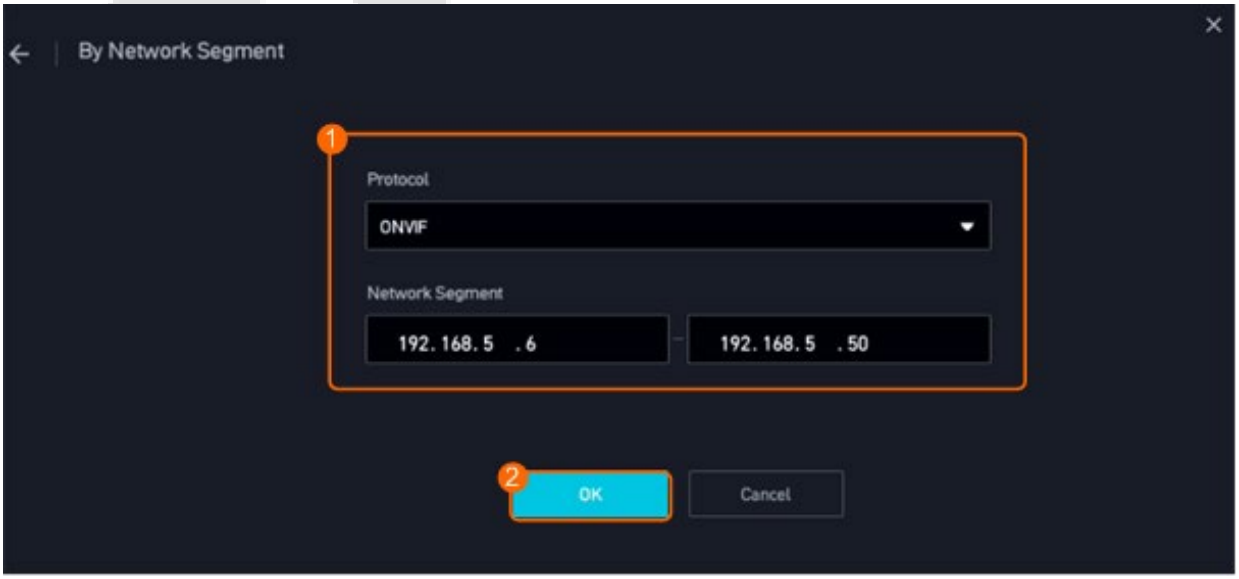
Step 2 Log in to the LDU as the **admin** user.

Step 3 Right-click on the desktop and choose **Camera Management**.

Step 4 Click **Add** and select **By Network Segment**, as shown in below.



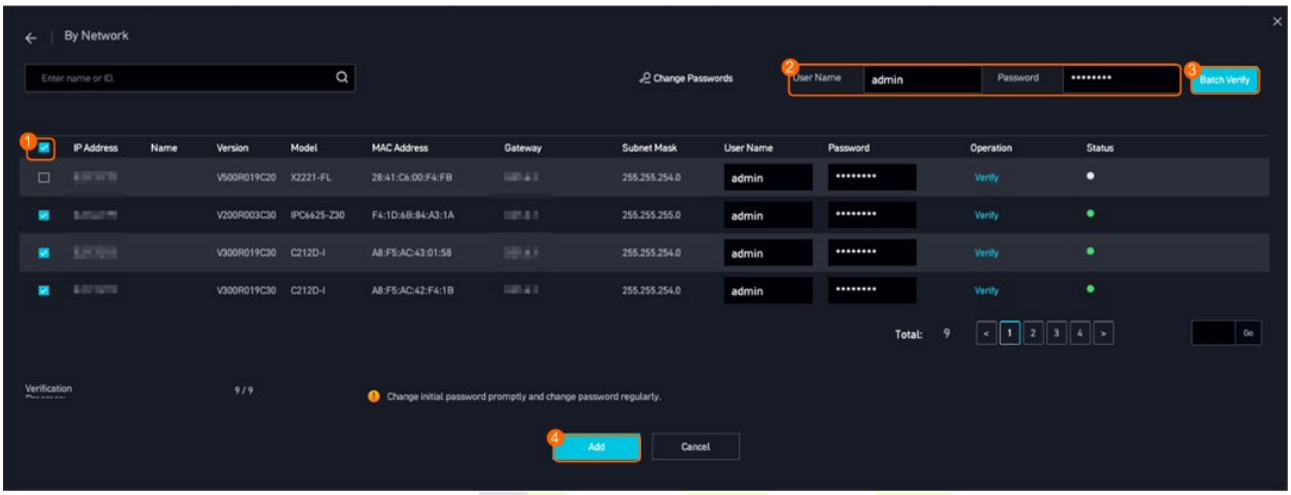
Step 5 Search for cameras, as shown in below.



Parameter Description

Parameter	Setting
Protocol	Select **ONVIF**.
Network Segment	Start and end IP addresses of the cameras. A precise network segment will shorten the search time.

Step 6 Verify cameras, as shown in below.



Parameter Description

Parameter	Description	Remarks
Change Passwords	Button for changing camera passwords in centralized mode on the device.	-
User Name/Password	User name and password for registering a camera.	-
Batch Verify	Button for verifying the registration user names and passwords of cameras in batches.	If the verification is passed, is displayed. If not, is displayed. If the user name or password of a camera has been changed after registration, the camera may fail the batch verification. You can configure the user name or password for the camera and then independently verify the camera.
Verify	Button for verifying the registration user name and password of a single camera.	

7.1.2.2 One by One

Step 1 Enable the ONVIF protocol on the camera side.

a. Log in to the camera web system as the **admin** user.

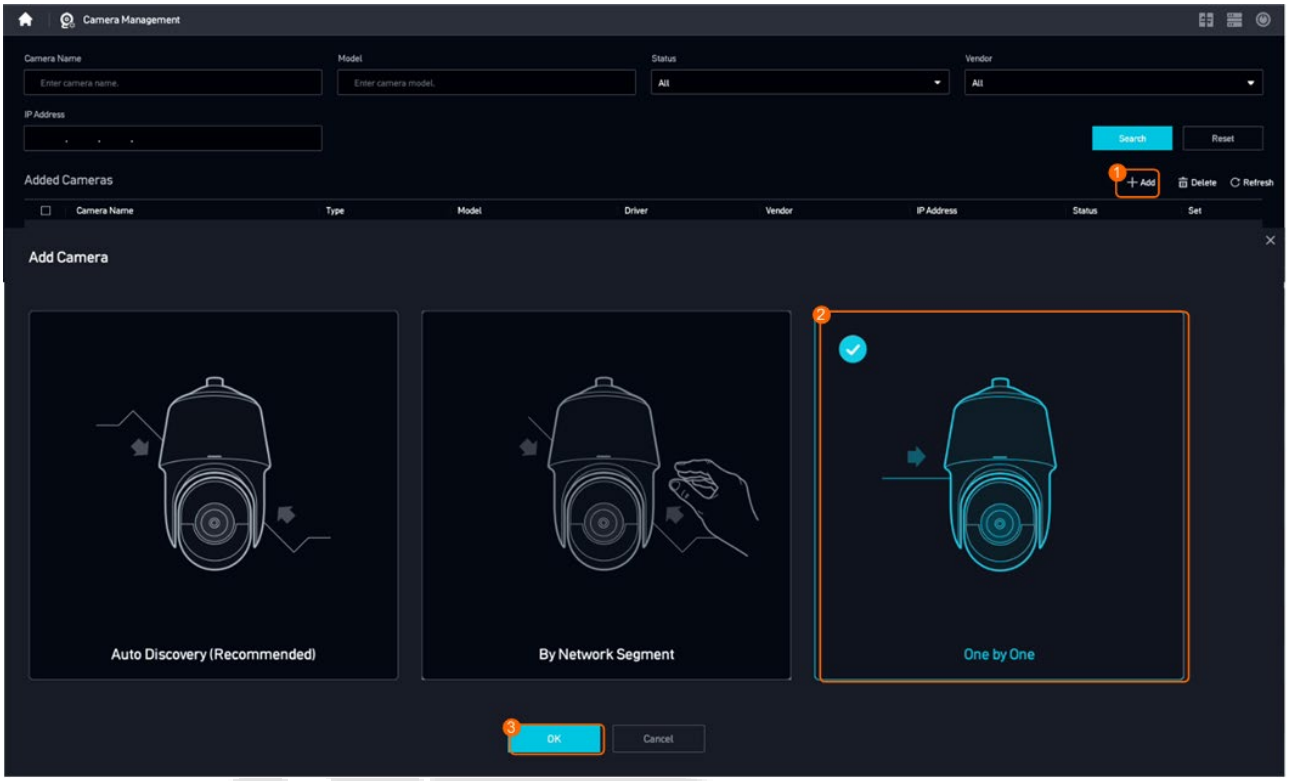
b. Choose **Settings** > **Network** > **Platform Connection** > **Second Protocol Parameters**.

c. Select **Enable ONVIF**.

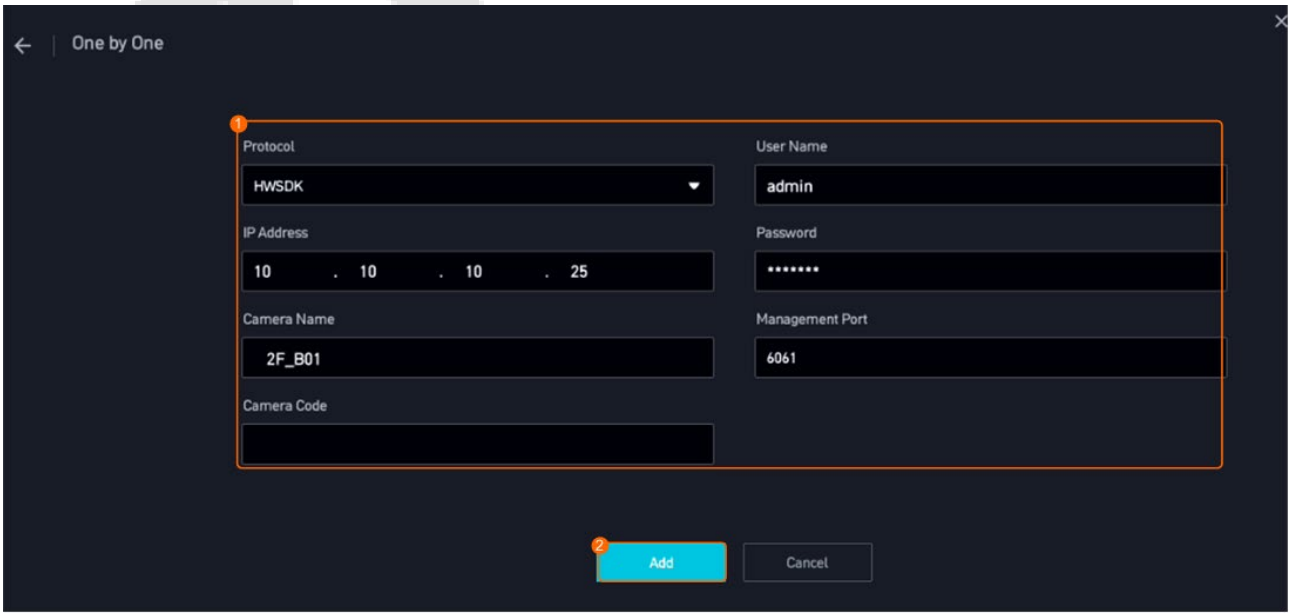
Step 2 Log in to the LDU as the **admin** user.

Step 3 Right-click on the desktop and choose **Camera Management**.

Step 4 Click **Add** and select **One by One**, as shown in below.



Step 5 Add one camera, as shown in below.



Note: The following table describes the parameters. You only need to set the parameters listed here.

Parameter Description

Parameter	Description
Protocol	Select **ONVIF**.
IP Address	Camera IP address. Set it based on the site requirements.
Camera Name	Camera name. Customize the name.
User Name/Password	-
Management Port	You do not need to set this parameter. After you select a protocol, the default port number is automatically generated.

7.1.3 GB/T 28181-based Access

Context

- GB/T 28181-compliant cameras can be connected to the AS1700 in only one mode illustrated in table below.

Application Scenarios

Mode	Application Scenario	Remarks
One by One	The device can be connected to the **network where the IP addresses of the cameras are located**. The network cables can be connected to the network ports corresponding to the same VLAN or different VLANs.	Log in to the camera web system to configure camera IP addresses.

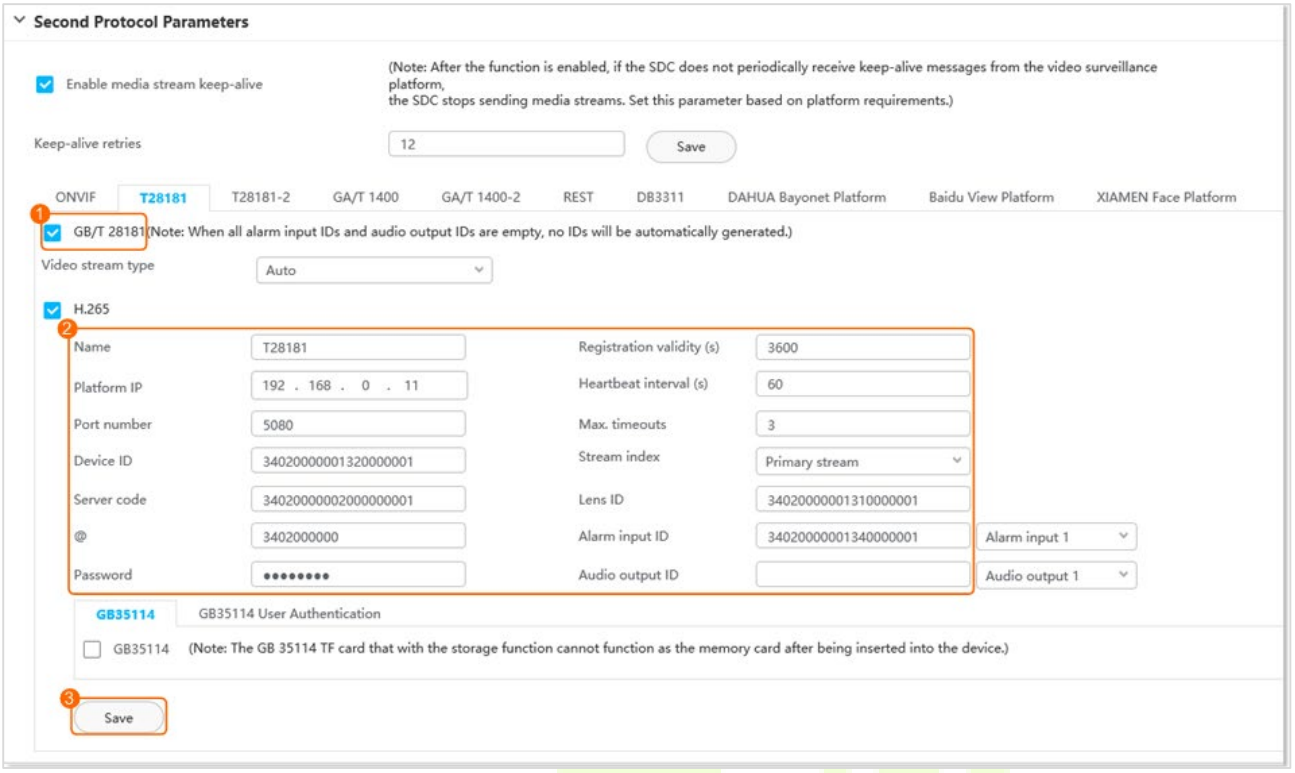
Procedure

Step 1 Enable the GB/T 28181 protocol on the camera side.

a. Log in to the camera web system as the **admin** user.

b. Choose **Settings** > **Network** > **Platform Connection** > **Second Protocol Parameters** > **T28181**.

c. Set GB/T 28181 parameters, as shown in below.



Parameter Description

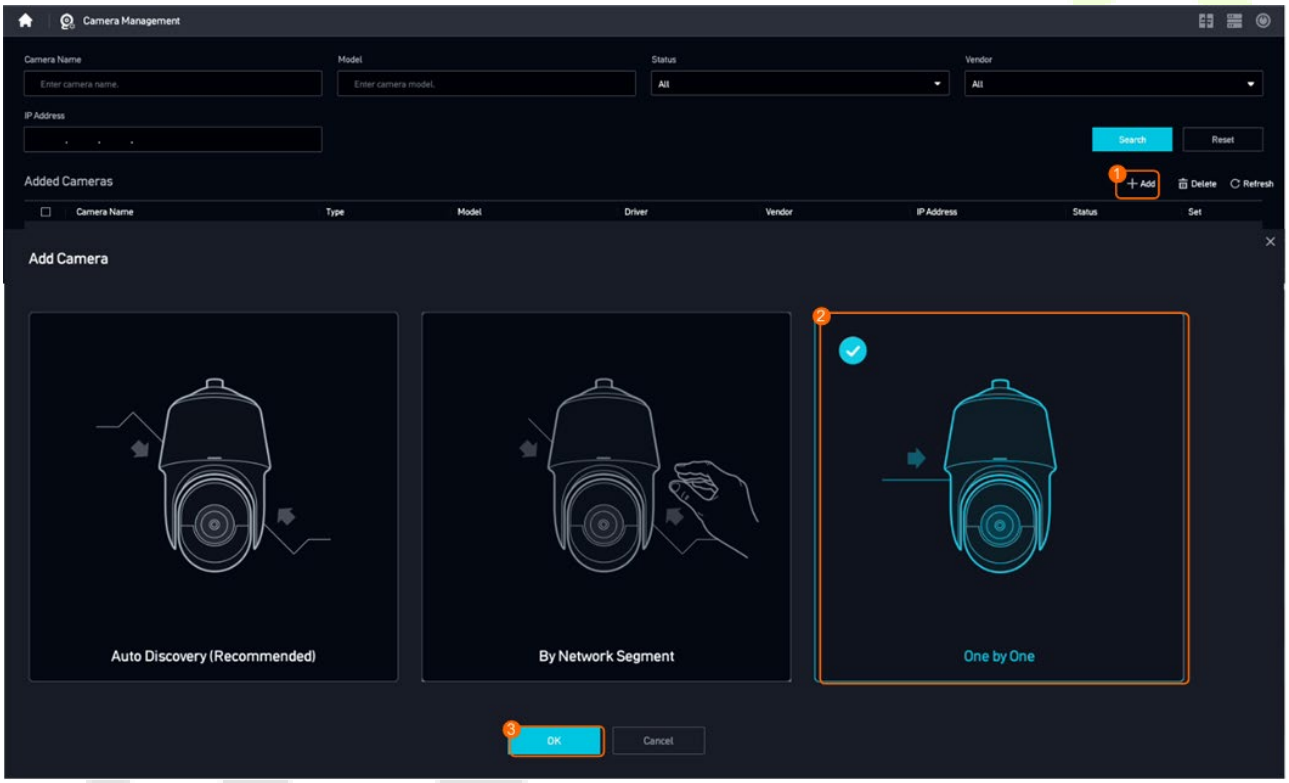
Parameter	Description
Name	Login name used to register a camera with the AS1700.
Platform IP	Enter the IP address of the AS1700 system.
Port number	GB/T 28181 port that the platform listens on. If the server and camera are on different networks and NAT is configured, set this parameter to the post-NAT port number.
Device ID	Unique device ID consisting of 20 digits. The eleventh to thirteenth digits must be 132.
Server code	GB/T 28181 server code. Enter a 20-digit string whose eleventh to thirteenth digits must be 200. Server codes must be the same for cameras connected to the same device.
SIP server domain	Domain name, which consists of 10 digits.
Password	Password used to register a camera with the platform. For security purposes, the password must consist of 8 to 20 characters and contain at least two types of the following characters: digits, letters, and special characters.
Lens ID	Lens ID, which must consist of 20 digits and the eleventh to thirteenth digits must be 131. Otherwise, you cannot view the live video in the AS1700 system.

Parameter	Description
Alarm input ID	Alarm input ID. The platform allocates it to a camera based on the device ID.
Audio output ID	Audio output ID. The platform allocates it to a camera based on the device ID.

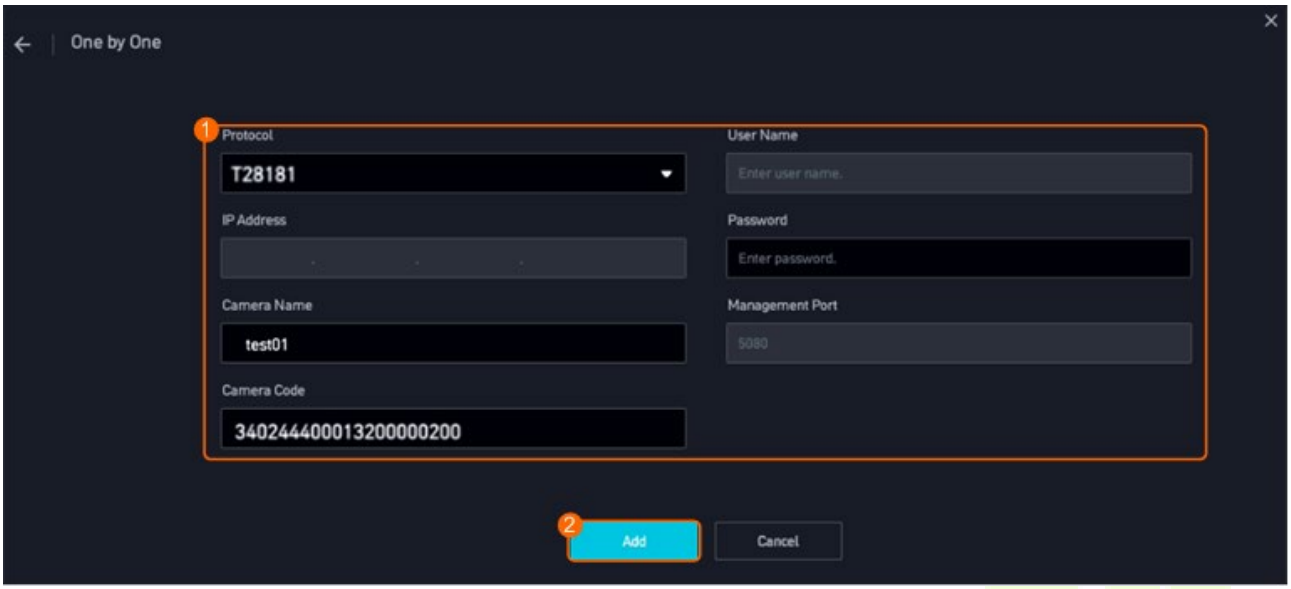
Step 2 Log in to the LDU as the **admin** user.

Step 3 Right-click on the desktop and choose **Camera Management**.

Step 4 Click **Add** and select **One by One**, as shown in below.



Step 5 Connect cameras one by one, as shown in below



Note: The following table describes the parameters. You only need to set the parameters listed here.

Parameter Description

Parameter	Description
Protocol	Select **T28181**.
Camera Name	Camera name. Customize the name.
Camera Code	Code and password of a camera. The code and password must be the same as the device ID and password configured in Step1.
Password	

7.2 PTZ Controls

7.2.1 Feature Description

Definition

- Users can control a PTZ device to adjust the shooting angle and focal length of a PTZ camera, widening the surveillance scope of cameras and improving video definition.

Customer Benefits

- Users can view live video from different angles, widening the surveillance scope and reducing hardware costs.
- Users can adjust the camera lens to a specified angle, improving operation efficiency.

Application Scenario

- When a suspicious person is detected, an operator can control the PTZ to view the live video of the suspicious person.

Application Limitations

Tour setting:

- Maximum number of tours supported by a camera: 8
- Maximum number of preset positions supported by a tour: 20
- Duration that a camera stays at each preset position: 3s to 3600s. The default value is 30s.
- Maximum number of tour plans that can be configured for each tour: 1
- Maximum number of tour plans that can be configured for a camera: 8

PTZ control interface:

- Number of PTZ rotation speed levels: 10
- Maximum number of preset positions supported by a single camera: The maximum number depends on the camera. In typical scenarios, the maximum number can be 128 or 256.
- Waiting duration range of the home position: 30s to 3600s. The default value is 300s.
- Automatic PTZ unlock duration range: 5s to 600s. The default value is 300s. The value 0 indicates that the PTZ is not automatically unlocked.
- PTZ control priority: There are 32 PTZ control priority levels for users to control the PTZ device when the PTZ device is locked. A smaller value indicates a higher priority. The value 1 indicates the highest priority. When the PTZ device is unlocked, the PTZ control priority is not distinguished.

The Micro Cloud does not support connection to network keyboards.

7.2.2 Feature Configuration

Context

- PTZ control functions include controlling PTZ cameras and setting preset positions and tours.
- If the invoked preset position is not a home position, the PTZ camera automatically rotates to the home position if no PTZ controls are performed before the configured waiting duration elapses.

Prerequisites

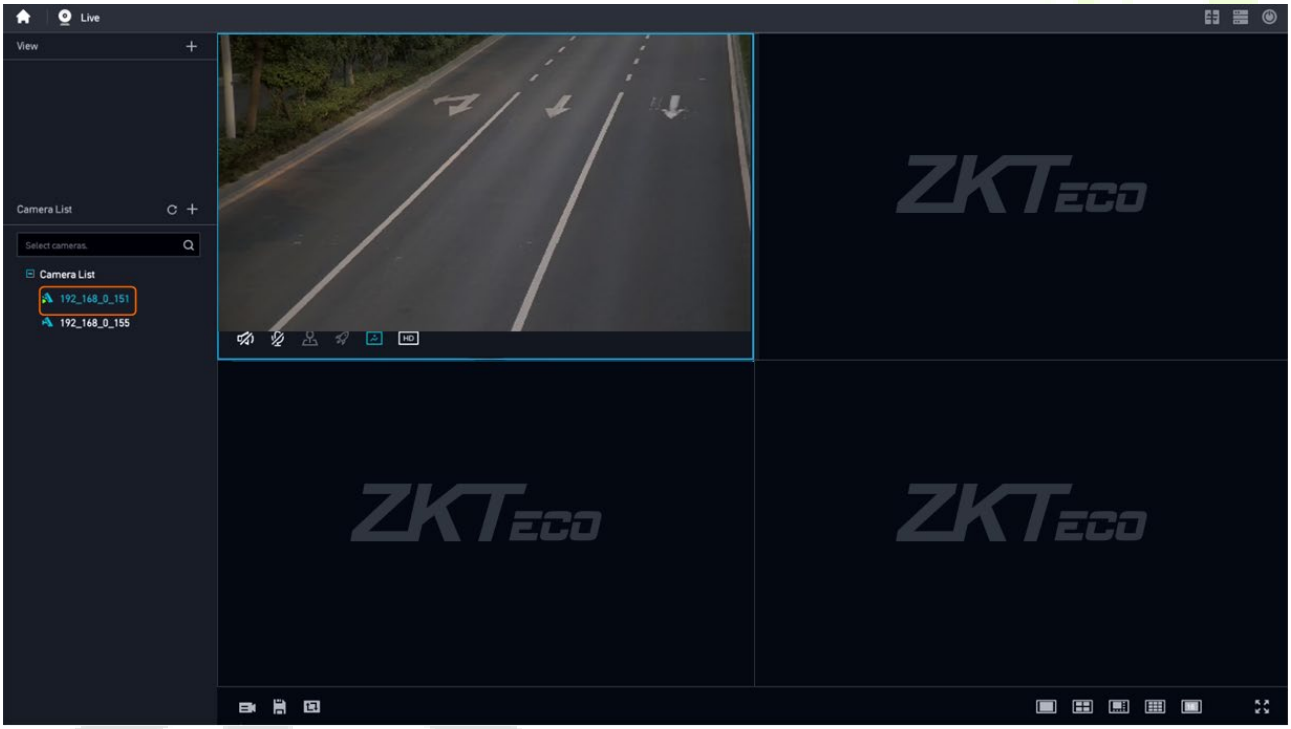
- The camera used is a PTZ dome camera or a camera of another type providing PTZ functions. The type configured for the camera used is the same as its actual type.
- This section uses a PTZ dome camera as an example.

7.2.3 Configuring Preset Positions and the Home Position

Procedure

Step 1 Log in to the LDU as the **admin** user.

Step 2 Drag a camera from the camera list to a live video pane, as shown in below.



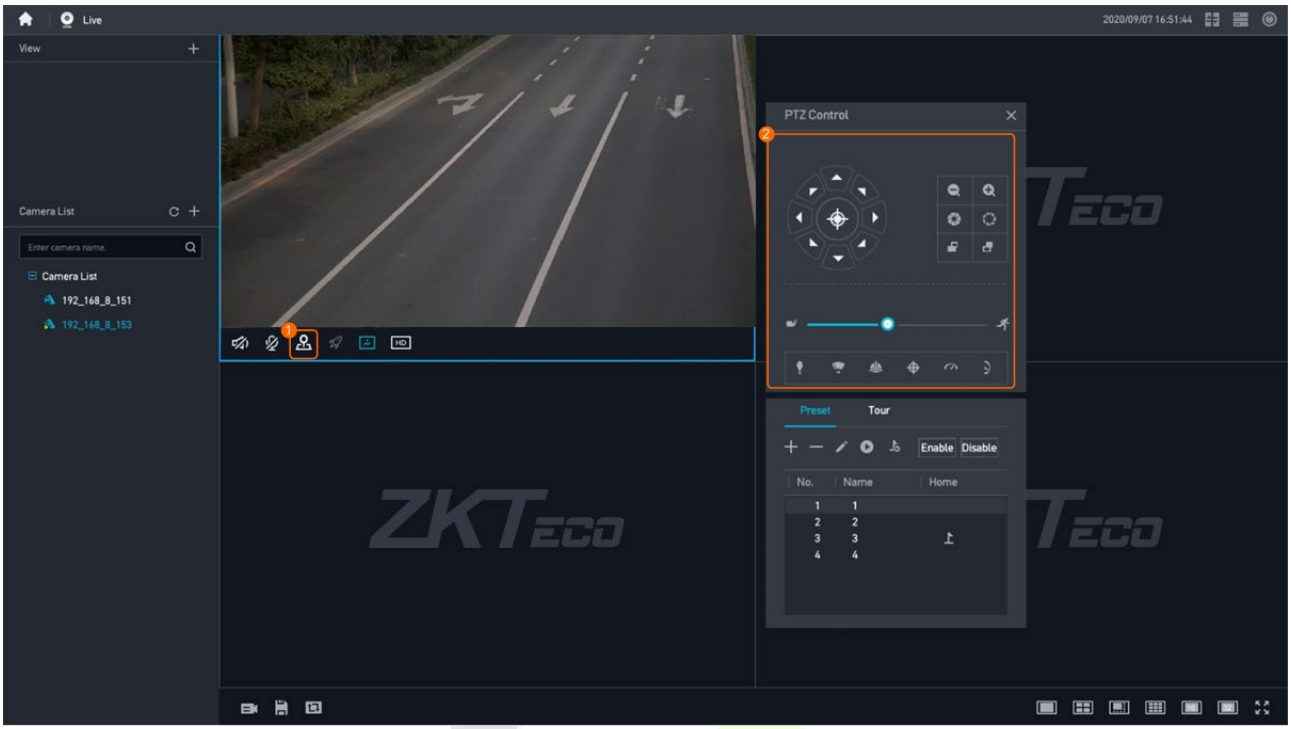
NOTE:

- Do not enable media security under **Camera Configuration** > **Video Settings** > **Extended Settings**. Otherwise, a blank screen may occur during live video viewing on the LDU.
- In the dual-screen scenario, the monitor connected to the HDMI2 port of the AS1700 is the primary screen by default, where you can perform operations such as GUI configuration. The monitor connected to the HDMI1 port of the AS1700 is the secondary screen, where you can view live video but cannot perform operations such as GUI configuration.

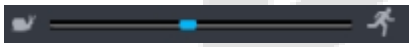
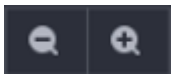
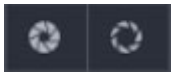
You can click in the upper right corner of the page to switch between the primary and secondary screens. After the switchover, the original primary screen becomes the secondary screen

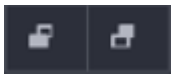
and only supports live video viewing. The original secondary screen becomes the primary screen and supports operations such as GUI configuration.

Step 3 Adjust the camera to a proper surveillance position, as shown in below.

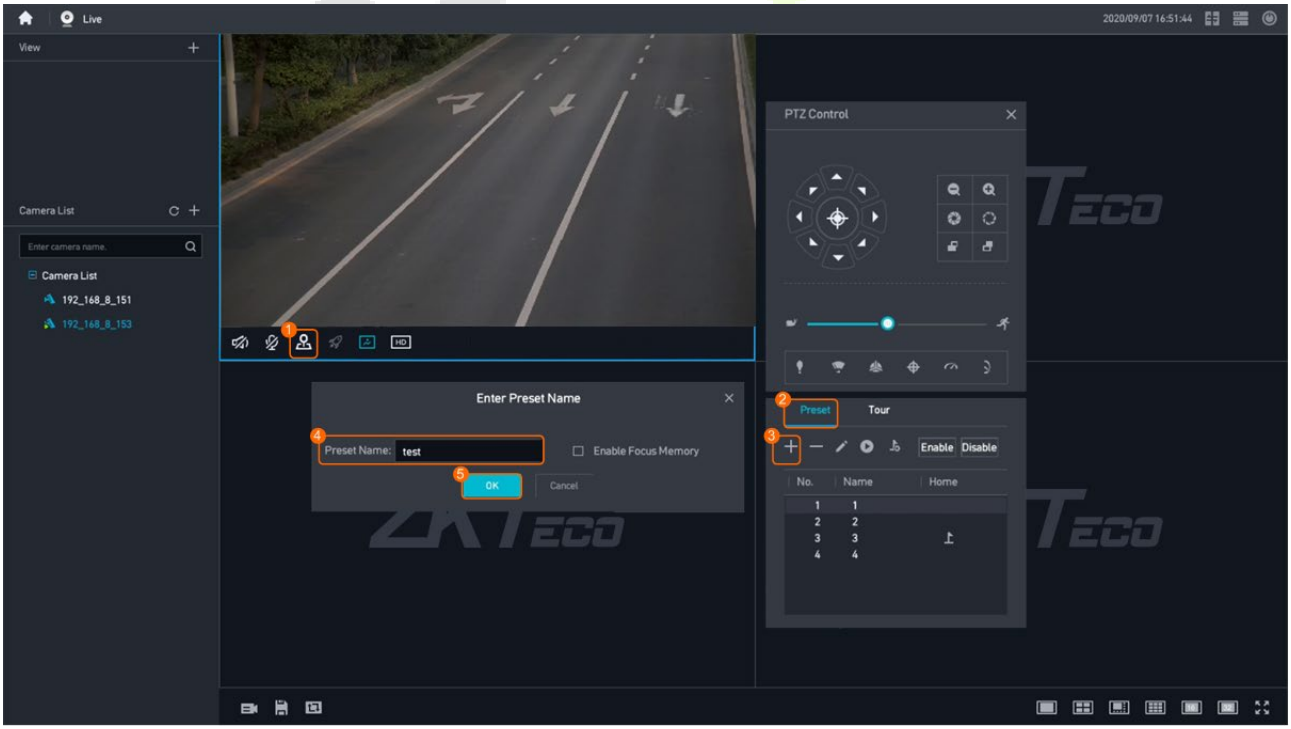


Function Description

Icon	Function
	Allows you to rotate the PTZ to adjust the camera shooting angle.
	Allows you to drag the slider to control the rotation speed and step of the PTZ. • Drag the speed slider to the left to decrease the rotation speed and step. • Drag the speed slider to the right to increase the rotation speed and step.
	Zooms in or out on the live video image.
	Increases or decreases the aperture.

Icon	Function
	Adjusts the focal length of the camera.
	Enables or disables the illuminator.
	Enables or disables the wiper.
	Rotates the PTZ to the home position.
	Quickly locates a position on the GUI through the intelligent 3D positioning function.
	Allows you to view live video from the camera that is performing a horizontal tour. The horizontal tour function allows unidirectional or back-and-forth scanning in either a clockwise or counter-clockwise direction at a specified degree (including 360°).
	Allows you to view live video from the camera that is performing a vertical tour. The vertical tour allows unidirectional or back-and-forth scanning in either a clockwise or counter-clockwise direction at a specified degree.

Step 4 Configure a preset position, as shown in below.

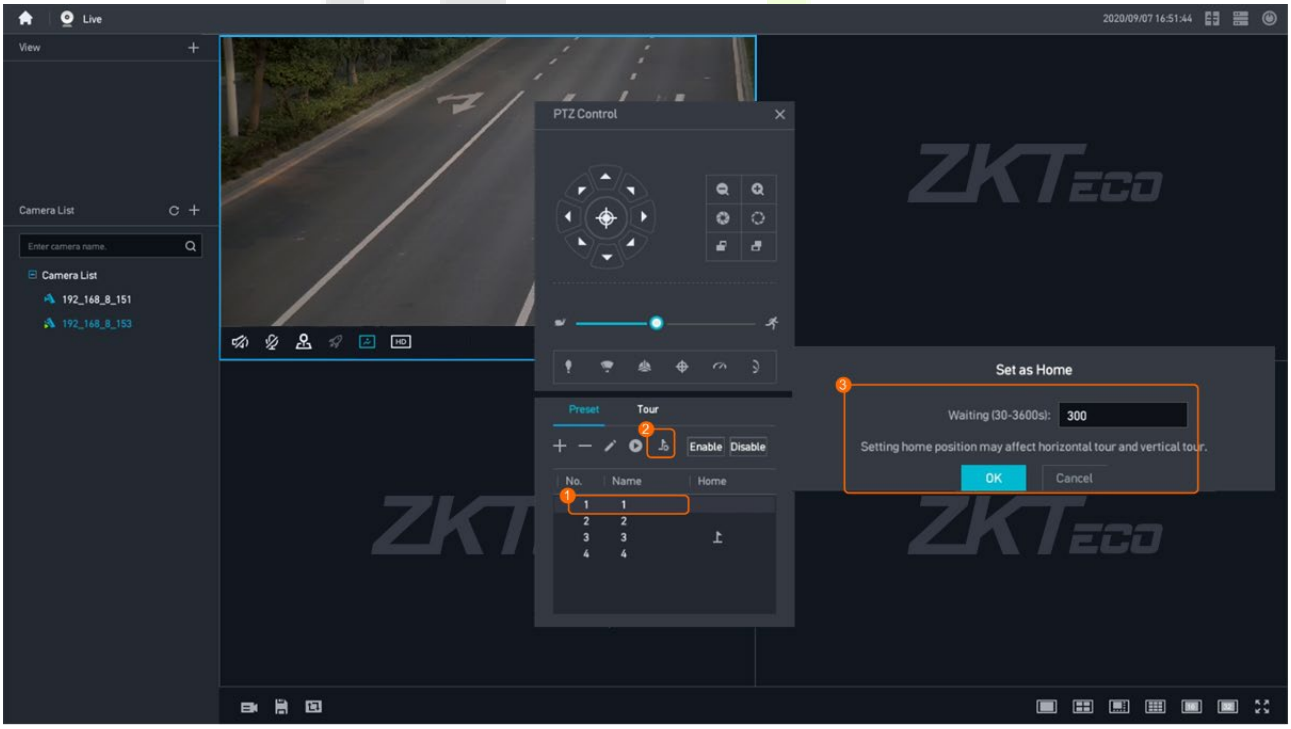


Parameter Description

Parameter	Setting
Preset Name	Set the name of a preset position as required.
Enable Focus Memory	If you need to frequently invoke preset positions, you are advised to select **Enable Focus Memory**. When a user invokes a preset position, the lens is switched to the preset position and automatically adjusts the focusing position so that the image will be clearer. However, if the lens frequently adjusts the focusing position, the lens life span will be shortened. When **Enable Focus Memory** is selected, the lens records the current focusing position. If you set the current position as a preset position, the camera does not automatically adjust the focusing position based on the image quality when the preset position is invoked later. Instead, the lens is directly switched to the recorded position. As a result, the image may be blurry. Determine whether to select **Enable Focus Memory** based on the site requirements.

Step 5 Repeat Step 3 through Step 4 to configure more preset positions. If you need to configure only one preset position, skip this step and go to the next step.

Step 6 Configure the home position, as shown in below.

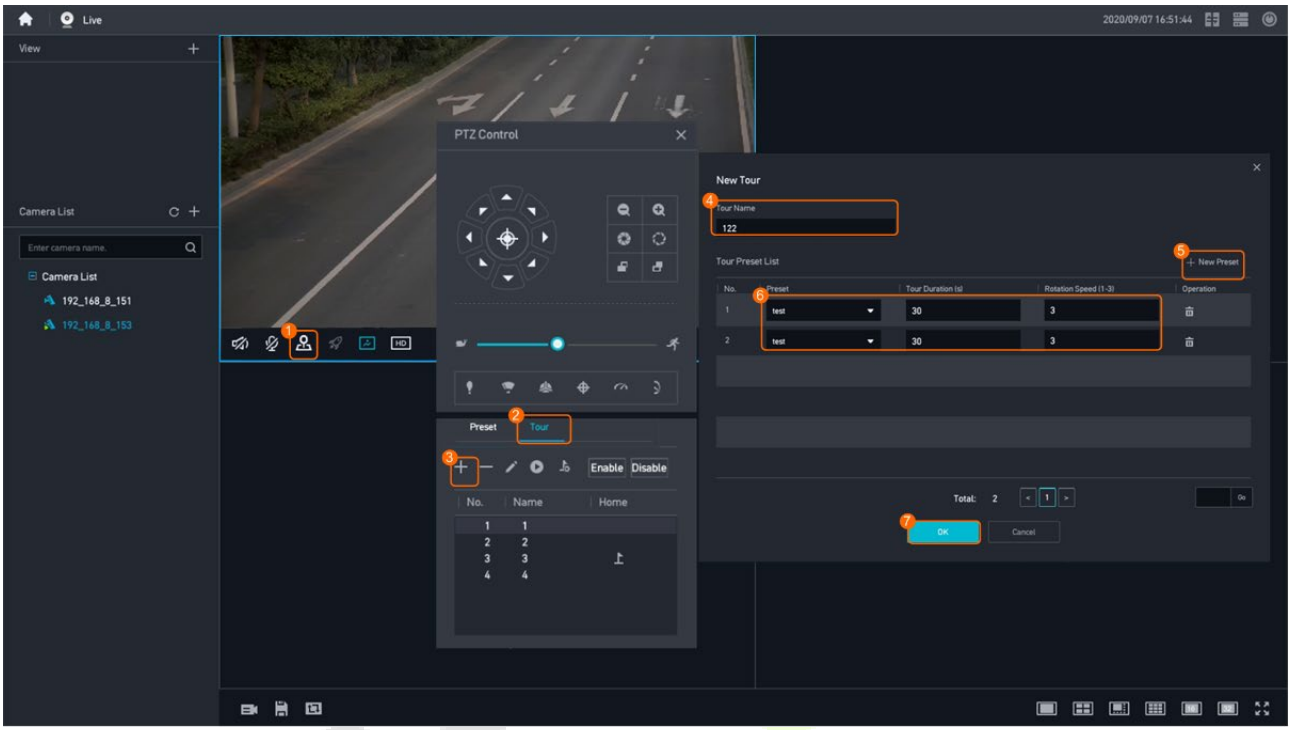


Step 7 After the home position is configured,  is displayed on corresponding preset positions.

7.2.4 Configuring a Tour and a Tour Plan

Procedure

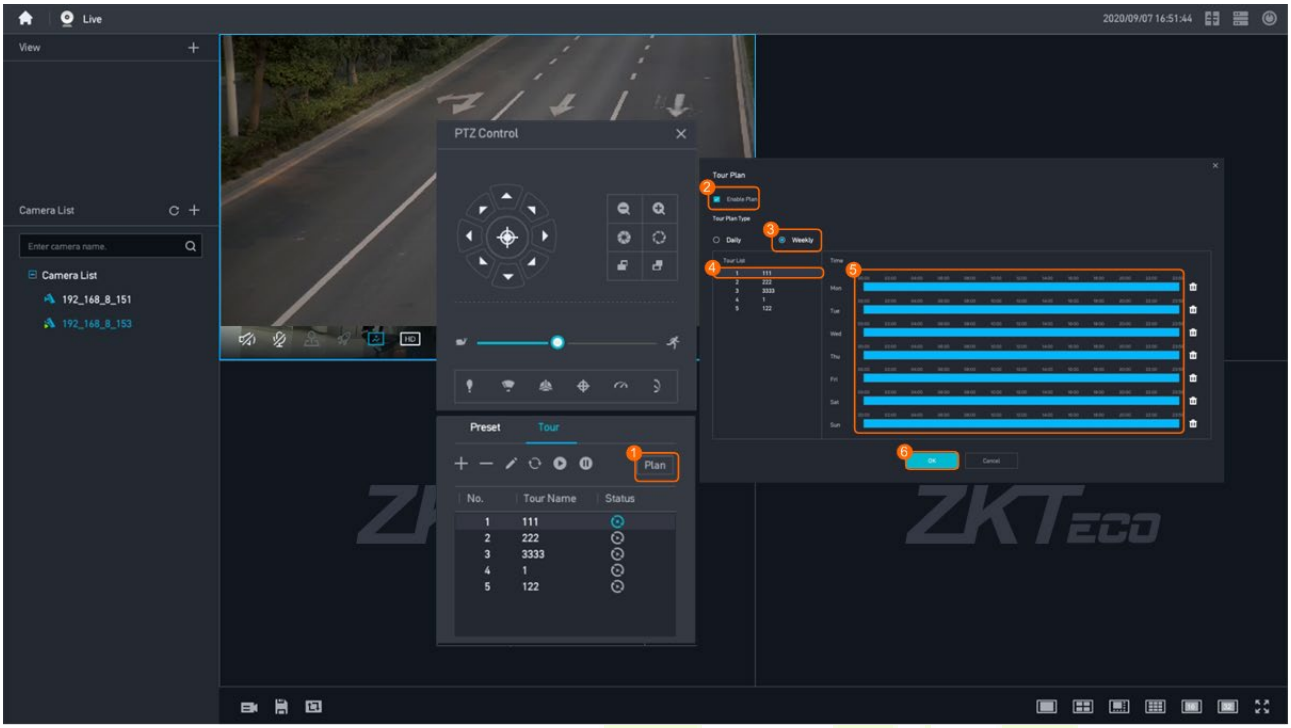
Step 1 Configure a tour, as shown in below.



Parameter and Button Description

Parameter/Button	Setting
Tour Name	Set the name of a tour as required.
Add Preset Position	Click this button to add a preset position. A minimum of two preset positions need to be added and a maximum of 20 preset positions are supported.
Preset	Select a preset position from the drop-down list box.
Tour Duration	Set the tour duration for each preset position. A short tour duration may shorten the service life of the camera motor and belt. If the preset positions do not need to be frequently switched onsite, you are advised to set the tour duration to be longer (for example, over 60 seconds).
Rotation Speed (1-10)	Set the tour speed for each preset position. The value ranges from 1 to 10, and the default value is **5**.

Step 2 Configure a tour plan, as shown in below.

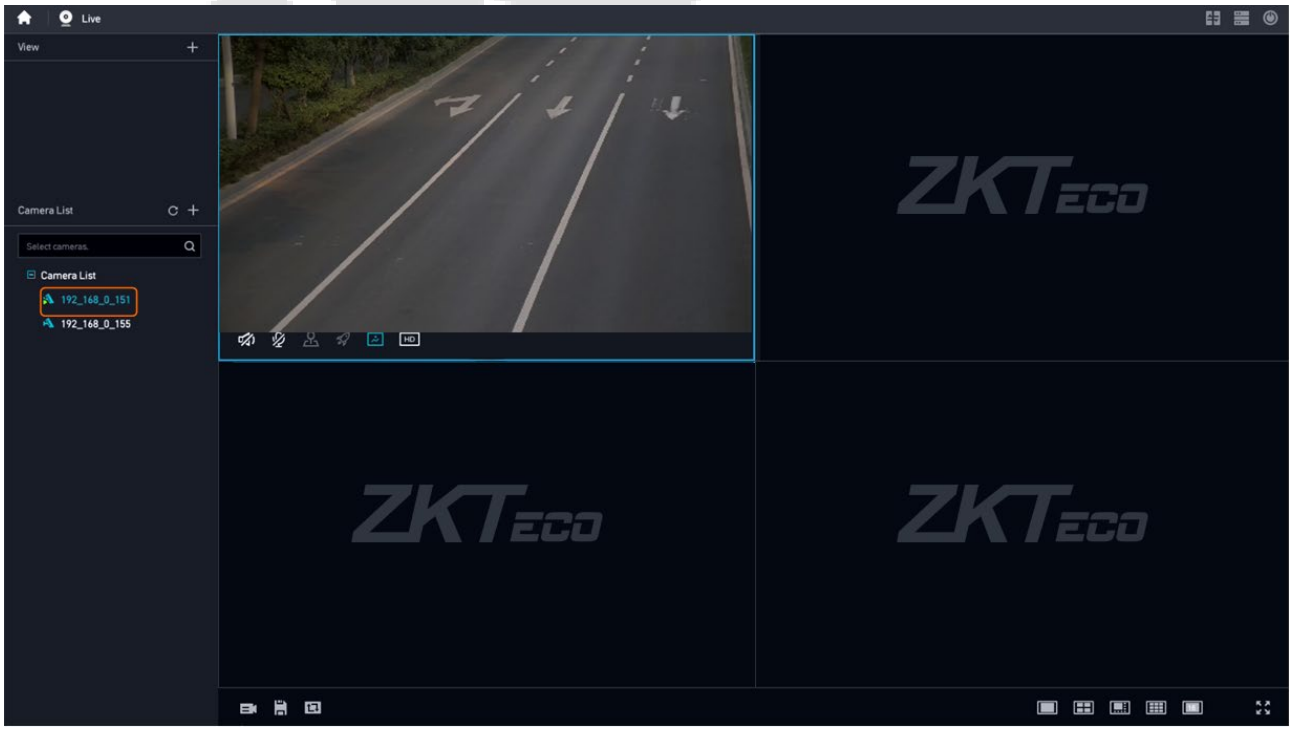


7.2.5 Verifying Preset Positions and the Home Position

Procedure

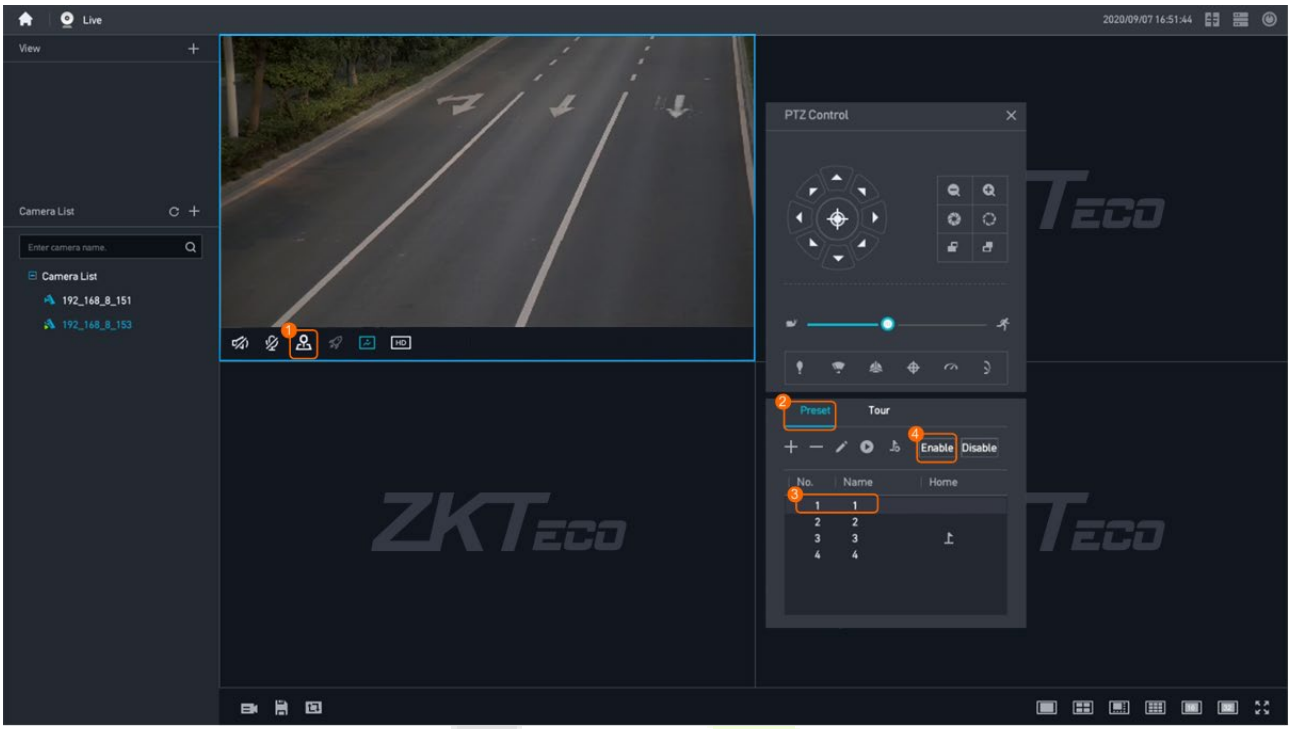
Step 1 Log in to the LDU as the **admin** user.

Step 2 Drag a camera from the camera list to a live video pane, as shown in below.



Step 3 Invoke a preset position, as shown in below.

The preset position is successfully invoked, and the camera rotates to the preset surveillance position.



Step 4 View the live video and check whether the camera rotates back to the home position after the duration specified by **Waiting Duration** in Step 6 in 7.2.3Configuring Preset Positions and the Home Position elapses.

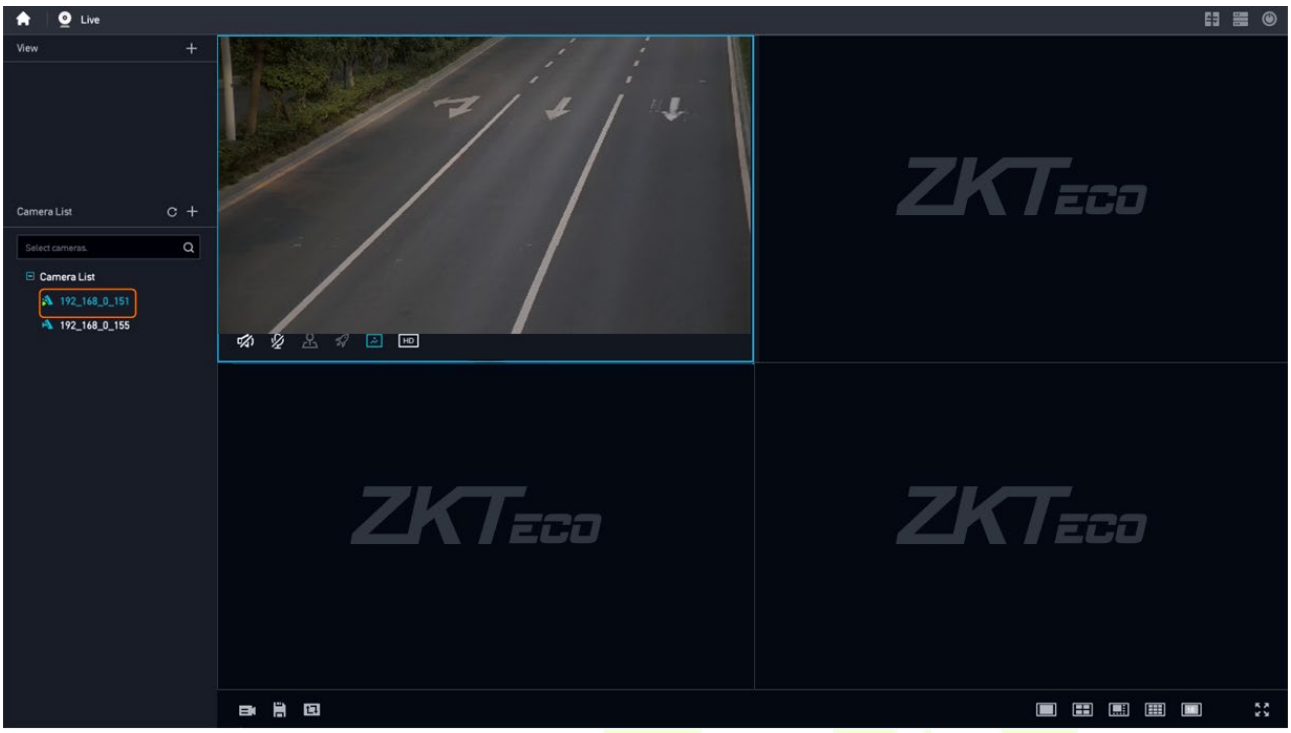
The home position must be different from the preset position. Otherwise, you cannot perceive image change in the live video.

7.2.6 Verifying a Tour and a Tour Plan

Procedure

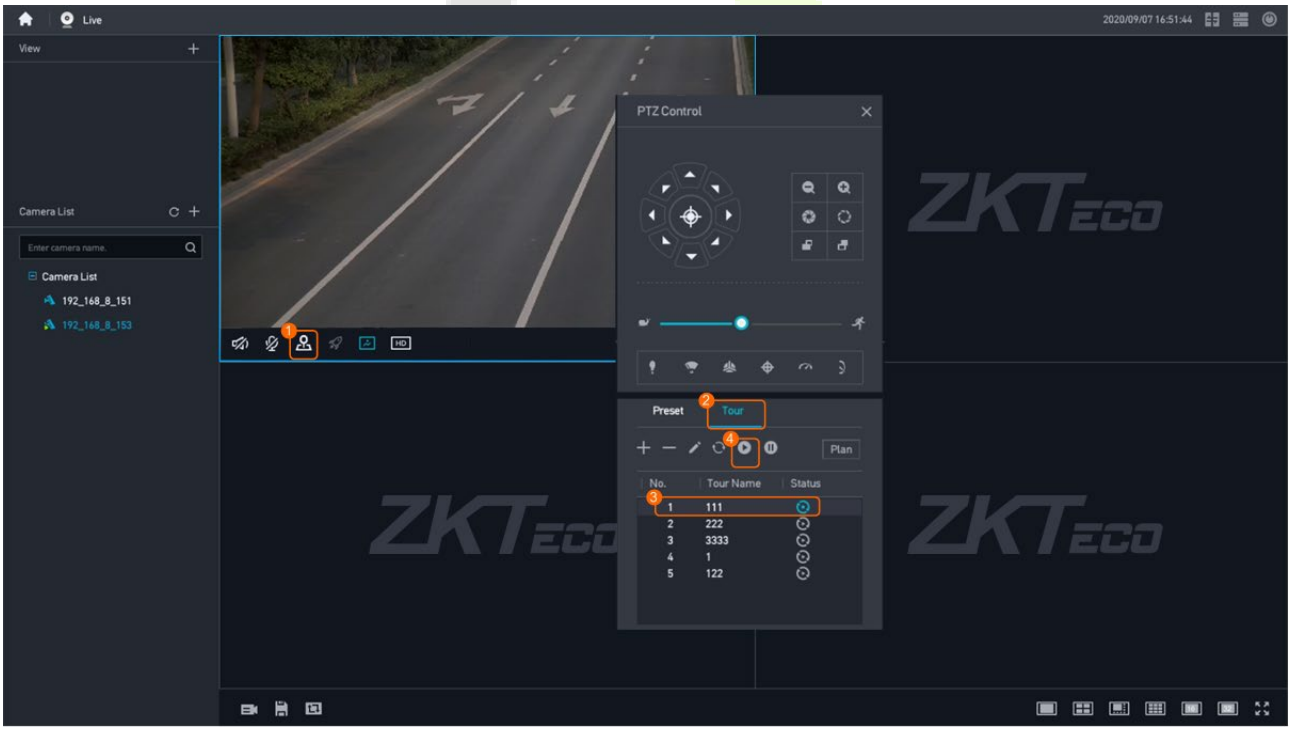
Step 1 Log in to the LDU as the **admin** user.

Step 2 Drag a camera from the camera list to a live video pane, as shown in below.



Step 3 Execute a tour, as shown in below.

The tour is successfully executed. The camera goes on the tour configured in Step 1 in 7.2.4 Configuring a Tour and a Tour Plan.



Step 4 Check whether the camera goes on the configured tour in the specified tour plan period on a day.

7.3 Intelligent 3D Positioning

7.3.1 Feature Description

Definition

- Users can zoom in on, zoom out on, and center the selected video image, quickly meeting viewing requirements.

Customer Benefits

- Users can view the details and surrounding environment, improving user experience.

Application Scenario

- An operator zooms in on the license plate of a vehicle in a video image to quickly recognize the license plate.

Application Limitations

- The camera must support the 3D positioning function.

7.3.2 Feature Configuration

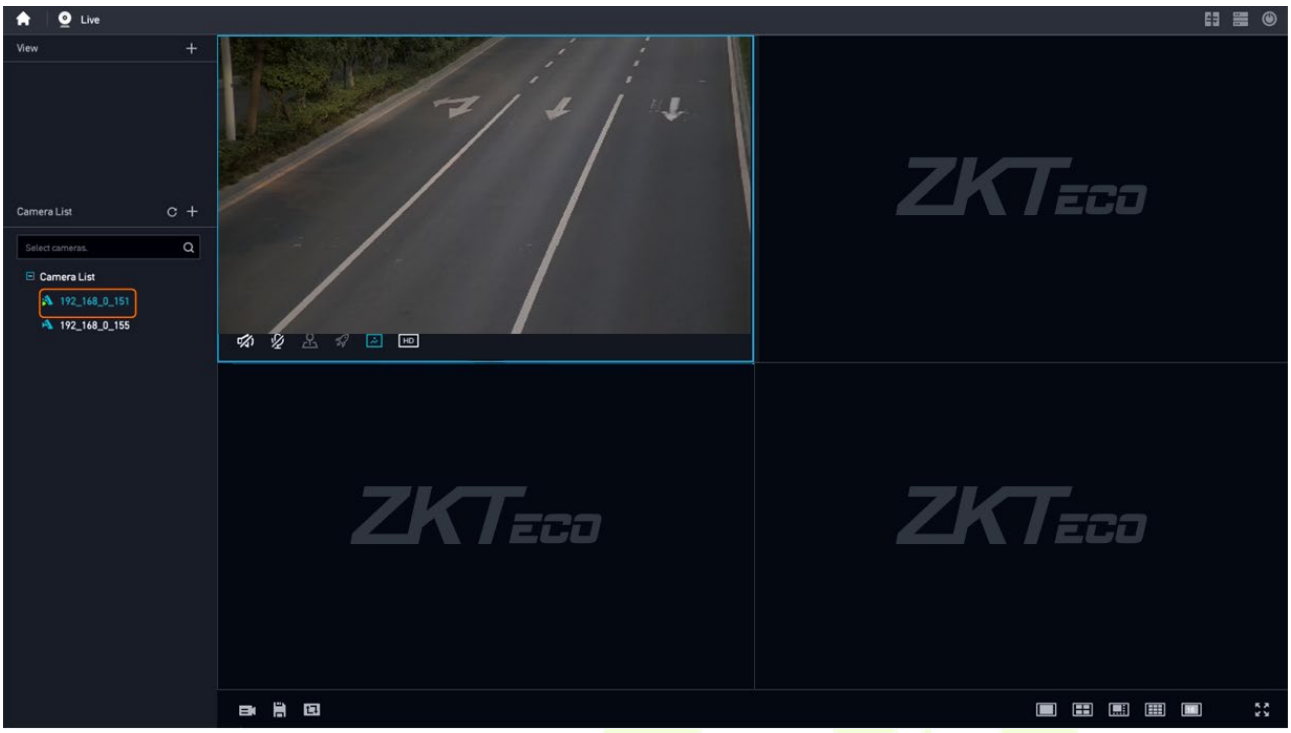
For details, see 4.1.1Configuring Real-Time Surveillance to complete the live preview configuration.

7.3.3 Feature Verification

Procedure

Step 1 Log in to the LDU as the **admin** user.

Step 2 Drag a camera from the camera list to a live video pane, as shown in below.

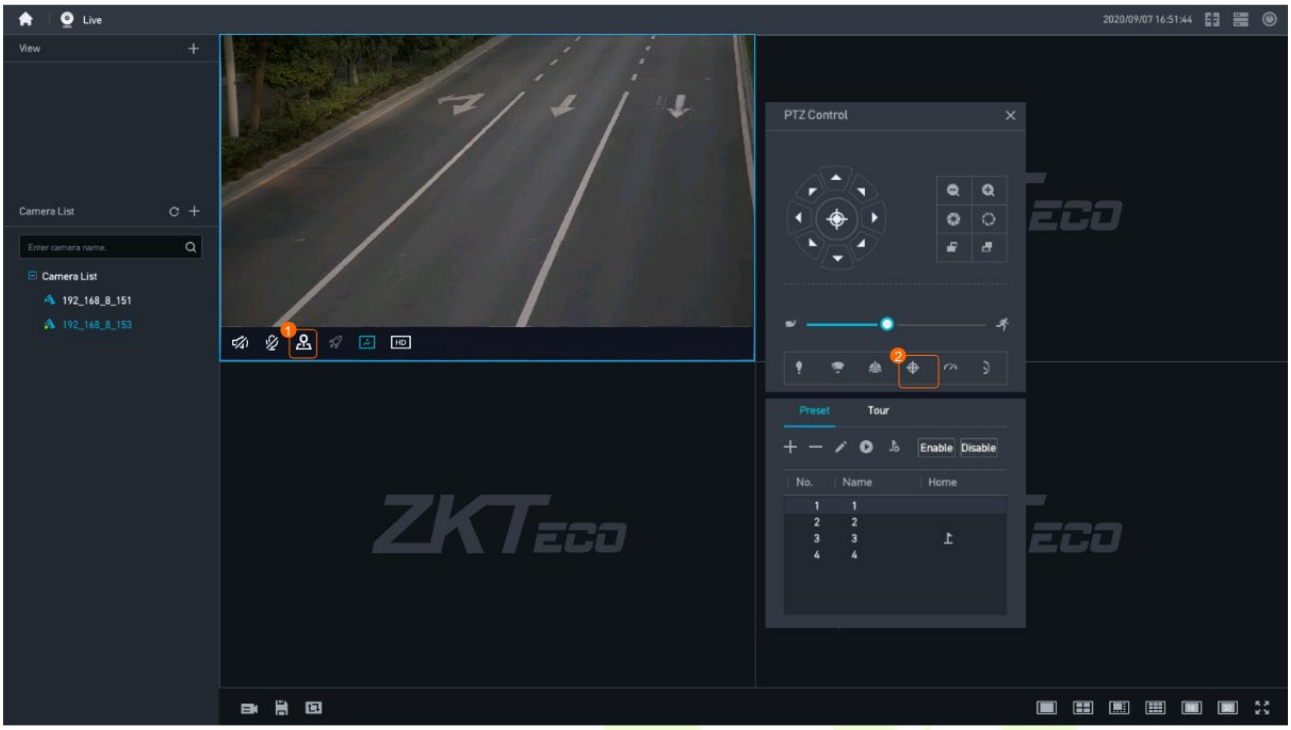


NOTE:

- Do not enable media security under **Camera Configuration** > **Video Settings** > **Extended Settings**. Otherwise, a blank screen may occur during live video viewing on the LDU.
- In the dual-screen scenario, the monitor connected to the HDMI2 port of the AS1700 is the primary screen by default, where you can perform operations such as GUI configuration. The monitor connected to the HDMI1 port of the AS1700 is the secondary screen, where you can view live video but cannot perform operations such as GUI configuration.

  You can click  in the upper right corner of the page to switch between the primary and secondary screens. After the switchover, the original primary screen becomes the secondary screen and only supports live video viewing. The original secondary screen becomes the primary screen and supports operations such as GUI configuration.

Step 3 Access the PTZ control page of the camera, as shown in below.



Step 4 Click to start 3D positioning.

- Zoom in an area and display it in the center.
  Users can drag a box from left to right on the live video image. The area inside the box is automatically zoomed in and displayed in the center of the video image.

- Zoom out an area and display it in the center.
  Users can drag a box from right to left on the live video image. The area inside the box is automatically zoomed out and displayed in the center of the video image.

- Center a position.
  You can click a position on the live video image. The camera rotates until the position becomes the center of the video image.

8 Troubleshooting

8.1 What Do I Do When a Blank Screen Occurs During Live Video Viewing on the LDU?

Symptom

- A blank screen occurs when a user views live video from a camera on the LDU.

Possible Causes

- **Media security** has been enabled for the camera.

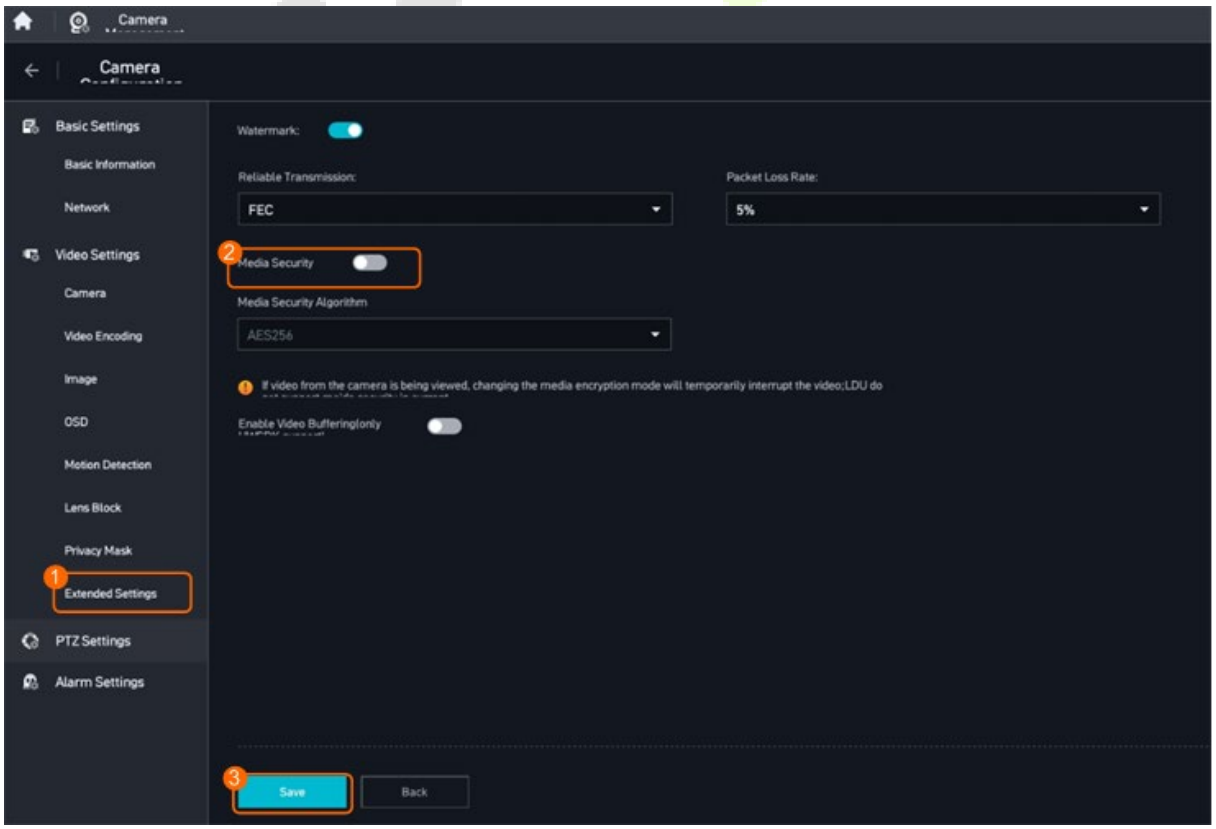
Solution

Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop to access the main menu, and choose **Camera Management**.

Step 3 Click ⚙ next to the specified camera.

Step 4 Disable media security, as shown in below.



8.2 Video Stutters When Live or Recorded Video Is Played on the LDU

Symptom

- After a camera that supports intelligent encoding is connected, video stuttering occurs during live or recorded video being played on the LDU.

Possible Causes

- The intelligent code function has been enabled for the camera on the LDU.

Solution

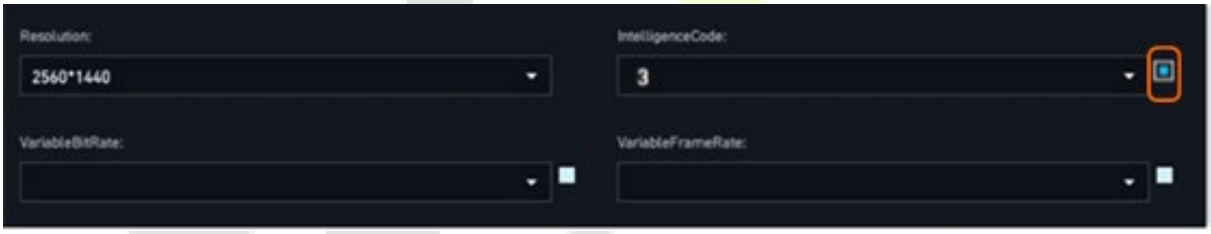
Step 1 Log in to the LDU as the **admin** user.

Step 2 Right-click on the desktop to access the main menu, and choose **Camera Management**.

Step 3 Click next to the camera whose video stutters.

Step 4 Choose **Video Settings** > **Video Encoding**.

Step 5 Check whether the radio button next to **IntelligenceCode** is selected, as shown in below.



- If so, go to **Step 6**.
- If not, contact technical support.

Step 6 Deselect the radio button next to **IntelligenceCode** and click **Save**.

Step 7 Check whether the fault is rectified.

- If the fault is rectified, no further action is required.
- If the fault persists, contact technical support.

8.3 Failure to Verify a Camera When You Follow the Wizard to Add It

Symptom

- When you attempt to add a camera by following the wizard, the verification fails repeatedly.

Possible Causes

- The user name and password configured for adding the camera are different from the actual ones.

  If the user name and password fail to be verified for five consecutive times, the system automatically locks the account for 5 minutes by default. During the lockout period, the camera cannot be added.

  The causes of the incorrect user name or password are as follows:

  - The user name and password are not changed, but either or both of them are incorrectly entered when you add the camera following the wizard. As a result, the verification fails.
  - The user name, password, or both have been changed. However, you still entered the old user name or password to add the camera. As a result, the verification fails.
- The camera software version is earlier than the required. In this version, the HWSDK protocol uses an insecure RSA encryption suite. By default, the device does not support connection to HWSDK-compliant cameras using the insecure RSA encryption suite.

Solution

- Wait for 5 minutes and enter the user name and password again.
  - If the camera is successfully added, no further action is required.
  - If the fault persists, the camera password may have been changed. You are advised to log in to the camera web page, reset the password, and add the camera again.

  The account may be locked again after multiple failed attempts. You are advised to wait for an account lockout period after changing the password. Then add the camera again.
- Log in to the AS1700 and disable the insecure RSA encryption suite.

  Enabling the insecure RSA encryption suite has security risks. You are advised to disable the insecure RSA encryption suite.

  a. Log in to the AS1700 as the **admin** user.

  b. Choose **Maintenance** > **Unified Configuration**.

  c. Set **HW_INIT_FORBID_RSA** to **0**, as shown in below.

8.4 Other Faults

Symptom	Possible Cause	Solution
The power button is unavailable.	The power button is damaged.	Contact the service provider.
The reset button is unavailable.	The reset button is damaged.	
The USB flash drive or mouse cannot be identified.	• The USB port is damaged. • The USB flash drive or mouse is damaged.	Insert a normal device into the port. For example, insert a normal mouse into the USB port. • If the fault persists, the device port is damaged. Replace the device and send the faulty device to the vendor for repair. • If the fault is rectified, the port device (such as the mouse) is damaged. Replace the port device.
The indicator of a network port is off, and online devices cannot be identified after network cables are connected.	• The network port is damaged. • The network cable is damaged.	
The display port has no output, and no image is displayed.	• The VGA or HDMI port is damaged. • The VGA or HDMI cable is damaged.	
No hard disk is detected.	• The hard disk port is damaged. • The data or power cable of the hard disk is damaged. • The hard disk is damaged.	
The audio port has no audio.	• The audio port is damaged. • The earphone or microphone is damaged.	

9 FQA

9.1 How Do I Restore a Device to Factory Settings?

Important Notes

CAUTION

- After factory settings are restored, all configuration data will be lost and the IP address and the user names and passwords of the operating system and service systems will be reset. Restore factory settings only when necessary.
- If you have upgraded the device software before this operation, the device software version change is as follows:
  - If the delivered software version of the device is V100R019C50, the software version changes to V100R019C50SPC100 after factory settings are restored.
  - If the delivered software version of the device is V100R019C50SPC100 or later, the software version changes to the delivered one after factory settings are restored.
- After factory settings are restored, the IP address, service user name, and password are as follows:
  - **IP address:** 192.168.3.111

Procedure

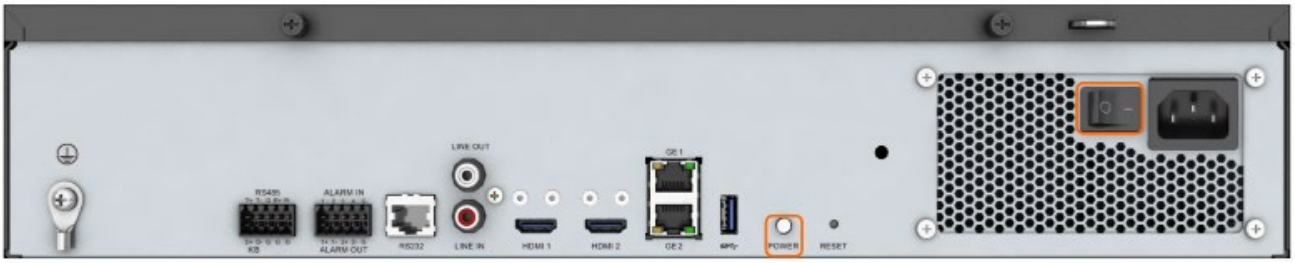
Step 1 Remove the network cable from the network port of the device to ensure that the device is disconnected from the network.

After the device is restored to factory settings, the default IP address changes to 192.168.3.111. If the network is not disconnected and the IP address 192.168.3.111 exists on the network, the factory setting restoration fails due to an IP address conflict.

Step 2 Ensure that the device is running, as shown in below.

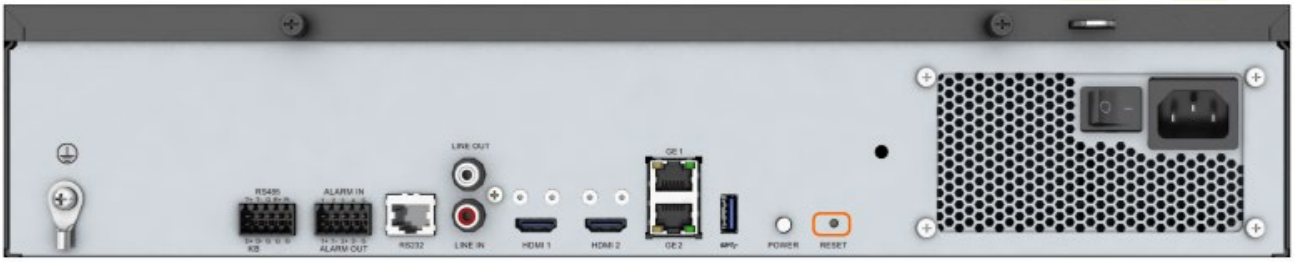
- The power switch is turned on (in I state).
- If the **POWER** button indicator is off, the device is in running state.

  If the **POWER** button indicator is steady blue, the device is in standby state.



Step 3 Use a needle-type object to press and hold down the **RESET** button for 10s, as shown in below.

The device automatically restarts after being restored to factory settings. It takes about 20 minutes to restore the device to factory settings.



Step 4 Log in to the LDU or AS1700 and configure initial service data, including setting the IP address and initializing hard disks.

- Perform this step on the LDU by referring to 3.2Configuring the Startup Wizard.
- In this scenario, ensure that the computer is directly connected to the device and is in the same network segment (192.168.3.111/24) as the device. Otherwise, the device will fail to be connected to the AS1700.

Step 5 Connect the network cable to the network port of the device to ensure that the device is connected to the network.

Appendix

Privacy Policy

Notice:

To help you better use the products and services of ZKTeco (hereinafter referred as "we", "our", or "us") a smart service provider, we consistently collect your personal information. Since we understand the importance of your personal information, we took your privacy sincerely and we have formulated this privacy policy to protect your personal information. We have listed the privacy policies below to precisely understand the data and privacy protection measures related to our smart products and services.

Before using our products and services, please read carefully and understand all the rules and provisions of this Privacy Policy. If you do not agree to the relevant agreement or any of its terms, you must stop using our products and services.

I. Collected Information

To ensure the normal product operation and help the service improvement, we will collect the information voluntarily provided by you or provided as authorized by you during registration and use or generated as a result of your use of services.

1. **User Registration Information:** At your first registration, the feature template (**Fingerprint template/Face template/Palm template**) will be saved on the device according to the device type you have selected to verify the unique similarity between you and the User ID you have registered. You can optionally enter your Name and Code. The above information is necessary for you to use our products. If you do not provide such information, you cannot use some features of the product regularly.

2. **Product information:** According to the product model and your granted permission when you install and use our services, the related information of the product on which our services are used will be collected when the product is connected to the software, including the Product Model, Firmware Version Number, Product Serial Number, and Product Capacity Information. **When you connect your product to the software, please carefully read the privacy policy for the specific software.**

II. Product Security and Management

1. When you use our products for the first time, you shall set the Administrator privilege before performing specific operations. Otherwise, you will be frequently reminded to set the Administrator privilege when you enter the main menu interface. **If you still do not set the Administrator privilege after receiving the system prompt, you should be aware of the possible security risk (for example, the data may be manually modified).**

2. All the functions of displaying the biometric information are disabled in our products by default. You can choose Menu > System Settings to set whether to display the biometric information. If you enable these functions, we assume that you are aware of the personal privacy security risks specified in the privacy policy.

3. Only your user ID is displayed by default. You can set whether to display other user verification information (such as Name, Department, Photo, etc.) under the Administrator privilege. **If you choose to display such information, we assume that you are aware of the potential security risks (for example, your photo will be displayed on the device interface).**

4. The camera function is disabled in our products by default. If you want to enable this function to take pictures of yourself for attendance recording or take pictures of strangers for access control, the product will enable the prompt tone of the camera. **Once you enable this function, we assume that you are aware of the potential security risks.**

5. All the data collected by our products is encrypted using the AES 256 algorithm. All the data uploaded by the Administrator to our products are automatically encrypted using the AES 256 algorithm and stored securely. If the Administrator downloads data from our products, we assume that you need to process the data and you have known the potential security risk. In such a case, you shall take the responsibility for storing the data. You shall know that some data cannot be downloaded for sake of data security.

6. All the personal information in our products can be queried, modified, or deleted. If you no longer use our products, please clear your personal data.

III. Others

You can visit https://www.zkteco.com/cn/index/Index/privacy_protection.html to learn more about how we collect, use, and securely store your personal information. To keep pace with the rapid development of technology, adjustment of business operations, and to cope with customer needs, we will constantly deliberate and optimize our privacy protection measures and policies. Welcome to visit our official website at any time to learn our latest privacy policy.

Eco-friendly Operation

The product's "eco-friendly operational period" refers to the time during which this product will not discharge any toxic or hazardous substances when used in accordance with the prerequisites in this manual.

The eco-friendly operational period specified for this product does not include batteries or other components that are easily worn down and must be periodically replaced. The battery's eco-friendly operational period is 5 years.

Hazardous or Toxic substances and their quantities

Component Name	Hazardous/Toxic Substance/Element					
	Lead (Pb)	Mercury (Hg)	Cadmium (Cd)	Hexavalent chromium (Cr6+)	Polybrominated Biphenyls (PBB)	Polybrominated Diphenyl Ethers (PBDE)
Chip Resistor	×	○	○	○	○	○
Chip Capacitor	×	○	○	○	○	○
Chip Inductor	×	○	○	○	○	○
Diode	×	○	○	○	○	○
ESD component	×	○	○	○	○	○
Buzzer	×	○	○	○	○	○
Adapter	×	○	○	○	○	○
Screws	○	○	○	×	○	○

○ indicates that the total amount of toxic content in all the homogeneous materials is below the limit as specified in SJ/T 11363—2006.

× indicates that the total amount of toxic content in all the homogeneous materials exceeds the limit as specified in SJ/T 11363—2006.

Note: 80% of this product's components are manufactured using non-toxic and eco-friendly materials. The components which contain toxins or harmful elements are included due to the current economic or technical limitations which prevent their replacement with non-toxic materials or elements.

ZKTeco Industrial Park, No. 32, Industrial Road,

Tangxia Town, Dongguan, China.

Phone : +86 769 - 82109991

Fax : +86 755 - 89602394

www.zkteco.com