Network Video Recorder

User's Manual

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V2.3.6

Foreword

General

This user's manual (hereinafter referred to be "the Manual") introduces the installation, functions and operations of the Network Video Recorder (NVR) devices (hereinafter referred to be "the Device"). Read carefully before using the Device, and keep the manual safe for future reference.

Safety Instructions

The following signal words might appear in the manual.

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

Revision History

Version	Revision Content	Release Time
V2.3.6	• Updated plug and play. • Updated live view. • Updated playback function. • Updated camera audio and remote warning light in AI functions. • Updated camera adding method. • Updated PTZ functions. • Updated initialization settings.	December 2023
V2.3.5	• Added 26 models. • Updated people counting. • Updated EPTZ linkage. • Updated AcuPick. • Updated camera encoding. • Added camera audio and remote warning light.	November 2023

Version	Revision Content	Release Time
V2.3.4	• Added PPE detection. • Added some models.	August 2023
V2.3.3	• Added smart object detection. • Added smart sound detection. • Added AcuPick function. • Added EPTZ linkage. • Updated live view control bar. • Updated modifying channel name. • Updated playback. • Updated port settings. • Added registration ID.	June 2023
V2.3.2	Added 14 models.	April 2023
V2.3.1	Added 8 models.	February 2023
V2.3.0	• Added NVR608H-32-XI/NVR608H-64-XI/ NVR608H-128-XI/NVR608RH-32-XI/ NVR608RH-64-XI/NVR608RH-128-XI. • Added smart tracking and sub screen mirroring.	August 2022
V2.2.0	Added AI SSA and Quick Pick.	June 2022
V2.1.0	Updated cluster service.	April 2022
V2.0.0	• Added intelligent diagnosis. • Added report query. • Added resetting password through DMSS app. • Added LLDP. • Updated several figures of the local page.	March 2022
V1.4.0	Added NVR11HS-W-S2-CE and NVR11HS-W-S2-FCC.	January 2022
V1.3.0	• Added some models. • Updated the web login page. • Added privacy masking. • Added AI codec.	November 2021
V1.2.0	Added NVR44-4KS2/I, NVR44-16P-4KS2/I, NVR48-4KS2/I, and NVR48-16P-4KS2/I.	June 2021
V1.1.0	Combined AI and non-AI models and deleted discontinued models.	May 2021
V1.0.10	Added several models.	April 2021
V1.0.9	Added 6 models.	February 2021
V1.0.8	Added 5 models.	January 2021
V1.0.7	• Added 2 models. • Added "5.11.7 Cellular Network".	August 2020

Version	Revision Content	Release Time
V1.0.6	• Added picture search, picture search playback, disk health monitoring, and exporting and importing face database. • Updated AI search, human detection, configuration of face recognition, and display settings.	May 2020
V1.0.5	Added split tracking, main-sub tracking, analytics list, configuring video quality analytics, iSCSI, and cluster service.	May 2020
V1.0.4	• Added 16 models. • Added PoE status, switch, and display.	April 2020
V1.0.3	• New GUI baseline, replaces all pages. • Added AI functions.	July 2019
V1.0.2	Updated the description of rear panel.	May 2019
V1.0.1	• Added NVR 5216-16P-I and NVR5216-8P-I. Updated relevant info. • Updated icons on the rear panel. • Added video metadata function and non-motor vehicle detection function.	September 2018

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. If there is inconsistency between the manual and the actual product,
- We are not liable for any loss caused by the operations that do not comply with the manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please see our final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.

- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please see our final explanation.

Important Safeguards and Warnings

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

Transportation Requirements

Transport the Device under allowed humidity and temperature conditions.

Storage Requirements

Store the Device under allowed humidity and temperature conditions.

Installation Requirements

Stability Hazard

Possible result: The rack might fall down and cause serious personal injury.

Preventive measures (including but not limited to):

- Before extending the rack to the installation position, read the installation instructions.
- When the Device is installed on the slide rail, do not place any load on it.
- Do not retract the slide rail while the Device is installed on it.

- Rotating Fan Blades Hazard

  Avoid touching the fan blades, especially when they are moving.
- Before installation, disconnect all the power cords.
- Do not connect the power adapter to the Device while the adapter is powered on.
- Strictly comply with the local electric safety code and standards. Make sure the ambient voltage is stable and meets the power supply requirements of the Device.
- Use the power adapter and cables provided with the Device. We assume no responsibility for injuries or damage caused by using the incorrect power adapter and cables.

- Reliably ground the grounding terminal of the Device to improve safety. The grounding terminal differs depending on the device, and some devices do not have grounding terminals. Process the situation according to the device model.

- The Device must be installed in a location that only professionals can access. Non-professionals are not allowed to enter the installation area.
- The Device must be reliably grounded by professionals. They must install the grounding conductor in the building floor and verify the grounding connection of the output receptacle.
- Do not place the Device in a place exposed to sunlight or near heat sources.
- Keep the Device away from dampness, dust, and soot.
- Install the Device on a stable surface to prevent it from falling.
- Put the Device in a well-ventilated place, and do not block its ventilation.
- The Device is a class I electrical appliance. Make sure that the power supply of the Device is connected to a power socket with protective earthing.
- Use power cords that conform to your local requirements, and are rated specifications.
- Before connecting the power supply, make sure the input voltage matches the server power requirement.
- When installing the Device, make sure that the power plug can be easily reached to cut off the power.
- It is prohibited for non-professionals and unauthorized personnel to open the device casing.
- Affix the controller securely to the building before use.

Operation Requirements

DANGER

- The Device or remote control contains button batteries. Do not swallow the batteries due to the risk of chemical burns.

  Possible result: The swallowed button battery can cause serious internal burns and death within 2 hours.

  Preventive measures (including but not limited to):

  - Keep new and used batteries out of reach of children.
  - If the battery compartment is not securely closed, stop using the product immediately and keep out of reach of children.
  - Seek immediate medical attention if a battery is believed to be swallowed or inserted inside any part of the body.
- Battery Pack Precautions

  Preventive measures (including but not limited to):

  - Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.
  - Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.
  - Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.
  - Do not subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.

WARNING

Place the Device in a location that children cannot easily access.

- This is a class 1 laser device. You can only insert modules that meet the requirements of class 1 lasers.

- Do not drop or splash liquid onto the Device, and make sure that there is no object filled with liquid on the Device to prevent liquid from flowing into it.
- Put the Device in a well-ventilated place, and do not block its ventilation.
- Operate the Device within the rated range of power input and output.
- Do not disassemble the Device without professional instruction.
- Transport, use and store the Device under allowed humidity and temperature conditions.

Maintenance Requirements

DANGER

Replacing unwanted batteries with the wrong type of new batteries might result in explosion.

Preventive measures (including but not limited to):

- Replace unwanted batteries with new batteries of the same type and model to avoid the risk of fire and explosion.
- Dispose of the old batteries as instructed.

The appliance coupler is a disconnection device. Keep it at a convenient angle when using it. Before repairing or performing maintenance on the device, first disconnect the appliance coupler.

Table of Contents

Foreword I
Important Safeguards and Warnings V
1 Introduction 1
1.1 Overview 1
1.2 Features 1
2 Front Panel and Rear Panel 4
2.1 Front Panel 4
2.1.1 NVR41-4KS2/NVR41-P-4KS2/NVR41-8P-4KS2/NVR41-4KS2/L/NVR41-P-4KS2/L/NVR41-8P-4KS2/L/NVR21-4KS2/NVR21-P-4KS2/NVR21-8P-4KS2/NVR21-S3/NVR21-P-S3/NVR21-8P-S3/NVR21-4KS3/NVR21-P-4KS3/NVR21-8P-4KS3/NVR41-EI/NVR41-P-EI/NVR41-8P-EI/NVR41-4KS3/NVR41-P-4KS3/NVR41-8P-4KS3 Series 4
2.1.2 NVR11HS-S3H/NVR11HS-P-S3H/NVR11HS-8P-S3H/NVR41HS-4KS2/NVR41HS-P-4KS2/NVR41HS-8P-4KS2/NVR41HS-4KS2/L/NVR41HS-P-4KS2/L/NVR41HS-8P-4KS2/L/NVR21HS-4KS2/NVR21HS-P-4KS2/NVR21HS-8P-4KS2/NVR21HS-S3/NVR21HS-P-S3/NVR21HS-8P-S3/NVR21HS-4KS3/NVR21HS-P-4KS3/NVR21HS-8P-4KS3/NVR41HS-4KS3/NVR41HS-P-4KS3/NVR41HS-8P-4KS3 5
2.1.3 NVR52-4KS2/NVR52-8P-4KS2/NVR52-16P-4KS2/NVR42-4KS2/NVR42-P-4KS2/NVR42-8P-4KS2/NVR42-16P-4KS2/NVR42-4KS2/L/NVR42-P-4KS2/L/NVR42-8P-4KS2/L/NVR42-16P-4KS2/L/NVR5224-24P-4KS2/NVR54-4KS2/NVR54-16P-4KS2/NVR44-4KS2/NVR44-16P-4KS2/NVR44-4KS2/L/NVR44-16P-4KS2/L/NVR5424-24P-4KS2/NVR22-4KS2/NVR22-P-4KS2/NVR22-8P-4KS2/NVR22-4KS3/NVR22-P-4KS3/NVR22-8P-4KS3/NVR22-16P-4KS3/NVR52-8P-4KS2E/NVR52-16P-4KS2E/NVR54-16P-4KS2E/NVR42-4KS3/NVR42-P-4KS3/NVR42-8P-4KS3/NVR44-4KS3/NVR42-16P-4KS3 Series 6
2.1.4 NVR58-4KS2/NVR58-16P-4KS2/NVR48-4KS2/NVR48-16P-4KS2/NVR48-4KS2/L/NVR48-16P-4KS2/L/NVR58-16P-4KS2E/NVR48-4KS3 Series 8
2.1.5 NVR21-W-4KS2 Series 8
2.1.6 NVR21HS-W-4KS2/NVR11HS-W-S2-CE/NVR11HS-W-S2-FCC Series 9
2.1.7 NVR21-I/NVR21-I2/NVR21-P-I/NVR21-P-I2/NVR21-8P-I/NVR21-8P-I2 Series 10
2.1.8 NVR21HS-I/NVR21HS-I2/NVR21HS-P-I/NVR21HS-P-I2/NVR21HS-8P-I/NVR21HS-8P-I2/NVR44-4KS2/I/NVR44-16P-4KS2/I Series 11
2.1.9 NVR22-I/NVR22-I2/NVR22-P-I/NVR22-P-I2/NVR22-8P-I/NVR22-8P-I2/NVR22-16P-I/NVR22-16P-I2/NVR52-EI/NVR52-8P-EI/NVR52-16P-EI/NVR41HS-EI/NVR42-EI/NVR41HS-P-EI/NVR42-P-EI/NVR41HS-8P-EI/NVR42-8P-EI/NVR42-16P-EI/NVR44-EI/NVR44-16P-EI/NVR52-XI/NVR52-8P-XI/NVR52-16P-XI/NVR54-XI/NVR58-XI 12
2.1.10 NVR48-I/NVR58-I/NVR58-I/L Series 14
2.1.11 NVR42-I/NVR44-I/NVR54-I/NVR54-I/L/NVR52-I/NVR52-I/L Series 15
2.1.12 NVR48-4KS2/I/NVR48-16P-4KS2/I/NVR54-EI/NVR54-16P-EI/NVR58-EI/NVR58-16P-EI/NVR48-EI/NVR48-16P-EI 15
2.1.13 NVR608-32-4KS2 Series 16
2.1.14 NVR608-64-4KS2/NVR608-128-4KS2/NVR608H-XI/NVR608RH-XI Series 17
2.1.15 NVR616-4KS2/NVR616-XI/NVR50-EI Series 18
2.1.16 NVR624-XI Series 20
2.2 Rear Panel 22

2.2.1 NVR21-4KS2/NVR21-P-4KS2/NVR21-8P-4KS2/NVR21-4KS3/NVR21-P-4KS3/NVR21-8P-4KS3/NVR41-EI/NVR41-8P-EI/NVR41-P-EI/NVR41-4KS3/NVR41-P-4KS3/NVR41-8P-4KS3 Series 22
2.2.2 NVR11HS-S3H/NVR11HS-P-S3H/NVR11HS-8P-S3H/NVR21HS-4KS2/NVR21HS-P-4KS2/NVR21HS-8P-4KS2/NVR41HS-4KS2/NVR41HS-P-4KS2/NVR41HS-8P-4KS2/NVR41HS-4KS2/L/NVR41HS-P-4KS2/L/NVR41HS-8P-4KS2/L/NVR21HS-S3/NVR21HS-P-S3/NVR21HS-8P-S3/NVR21HS-4KS3/NVR21HS-P-4KS3/NVR21HS-8P-4KS3/NVR41HS-EI/NVR41HS-P-EI/NVR41HS-8P-EI/NVR41HS-4KS3/NVR41HS-P-4KS3/NVR41HS-8P-4KS3 24
2.2.3 NVR22-4KS2/NVR22-P-4KS2/NVR22-8P-4KS2//NVR22-4KS3/NVR22-P-4KS3/NVR22-8P-4KS3/NVR22-16P-4KS3 Series 27
2.2.4 NVR52-4KS2/NVR52-8P-4KS2/NVR52-16P-4KS2/NVR52-24P-4KS2/NVR52-8P-4KS2E/NVR52-16P-4KS2E/NVR52-EI/NVR52-8P-EI/NVR52-16P-EI/NVR42-16P-EI Series 29
2.2.5 NVR52-XI/NVR52-8P-XI/NVR-52-16P-XI Series 32
2.2.6 NVR54-4KS2/NVR58-4KS2/NVR54-16P-4KS2/NVR58-16P-4KS2/NVR54-24P-4KS2/NVR58-16P-4KS2E 34
2.2.7 NVR41-4KS2/NVR41-P-4KS2/NVR41-8P-4KS2/NVR41-4KS2/L/NVR41-P-4KS2/L/NVR41-8P-4KS2/L/NVR21-S3/NVR21-P-S3/NVR21-8P-S3 37
2.2.8 NVR42-4KS2/NVR42-P-4KS2/NVR42-8P-4KS2/NVR42-16P-4KS2/NVR42-4KS2/L/NVR42-P-4KS2/L/NVR42-8P-4KS2/L/NVR42-16P-4KS2/L/NVR42-EI/NVR42-P-EI/NVR42-8P-EI/NVR42-4KS3/NVR42-P-4KS3/NVR42-8P-4KS3/NVR42-16P-4KS3 Series 38
2.2.9 NVR44-4KS2/NVR44-16P-4KS2/NVR44-4KS2/L/NVR44-16P-4KS2/L/NVR44-4KS2/I/NVR44-16P-4KS2/I/NVR48-EI/NVR44-EI/NVR48-16P-EI/NVR44-16P-EI/NVR44-4KS3/NVR48-4KS3 Series 40
2.2.10 NVR48-4KS2/NVR48-16P-4KS2/NVR48-4KS2/L/NVR48-16P-4KS2/L/NVR48-4KS2/I/NVR48-16P-4KS2/I Series 43
2.2.11 NVR21-W-4KS2 Series 45
2.2.12 NVR21HS-W-4KS2 47
2.2.13 NVR21-I/NVR21-I2 Series 48
2.2.14 NVR22-I/NVR22-I2 Series 49
2.2.15 NVR21-P-I/NVR21-P-I2 Series 50
2.2.16 NVR22-P-I/NVR22-P-I2 Series 51
2.2.17 NVR21-8P-I/NVR21-8P-I2 Series 53
2.2.18 NVR22-8P-I/NVR22-8P-I2 Series 54
2.2.19 NVR22-16P-I/NVR22-8P-I2 Series 55
2.2.20 NVR21HS-I/NVR21HS-I2 Series 57
2.2.21 NVR21HS-P-I/NVR21HS-P-I2 Series 58
2.2.22 NVR21HS-8P-I/NVR21HS-8P-I2 Series 59
2.2.23 NVR4208-8P-I Series 60
2.2.24 NVR4216-I Series 61
2.2.25 NVR58-I/NVR58-I/L/NVR48-I Series 62
2.2.26 NVR54-I/NVR54-I/L/NVR44-I Series 64
2.2.27 NVR52-16P-I/NVR52-16P-I/L/NVR52-8P-I/NVR52-8P-I/L/NVR42-16P-I Series 66
2.2.28 NVR608-4KS2/NVR608H-XI/NVR608RH-XI Series 69
2.2.29 NVR616-4KS2/NVR616-XI Series 71

2.2.30 NVR624-XI Series....73
2.2.31 NVR11HS-W-S2-CE/NVR11HS-W-S2-FCC Series....74
2.2.32 NVR54-EI/NVR54-16P-EI/NVR58-EI/NVR58-16P-EI/NVR54-XI/NVR-58-XI Series....75
2.2.33 NVR50-EI Series....78
2.3 Alarm Connection....79
2.3.1 Alarm Port....79
2.3.2 Alarm Input Port....80
2.3.3 Alarm Output Port....82
2.3.4 Alarm Relay Specifications....83
2.4 Two-way Talk....83
2.4.1 Device-end to PC-end....83
2.4.2 PC-end to the Device-end....84
3 Device Installation....85
3.1 Device Installation Diagram....85
3.2 Checking Unpacked NVR....86
3.3 HDD Installation....86
3.3.1 NVR41-4KS2/NVR41-P-4KS2/NVR41-8P-4KS2/NVR41-4KS2/L/NVR41-P-4KS2/L/NVR41-8P-4KS2/L/NVR21-4KS2/NVR21-P-4KS2/NVR21-8P-4KS2/NVR21-W-4KS2/NVR21-I/NVR21-I2/NVR21-P-I/NVR21-P-I2/NVR21-8P-I/NVR21-8P-I2/NVR21-S3/NVR21-P-S3/NVR21-8P-S3/NVR41-EI/NVR41-P-EI/NVR41-8P-EI....86
3.3.2 NVR41HS-4KS2/NVR41HS-P-4KS2/NVR41HS-8P-4KS2/NVR41HS-4KS2/L/NVR41HS-P-4KS2/L/NVR41HS-8P-4KS2/L/NVR21HS-4KS2/NVR21HS-P-4KS2/NVR21HS-8P-4KS2/NVR21HS-W-4KS2/NVR11HS-S3H/NVR11HS-P-S3H/NVR11HS-8P-S3H/NVR21HS-I/NVR21HS-I2/NVR21HS-P-I/NVR21HS-P-I2/NVR21HS-8P-I/NVR21HS-8P-I2/NVR21HS-S3/NVR21HS-P-S3/NVR21HS-8P-S3/NVR11HS-W-S2-CE/NVR11HS-W-S2-FCC/NVR41HS-EI/NVR41HS-P-EI/NVR41HS-8P-EI2....89
3.3.3 NVR22-8P-S2/NVR42-4KS2/NVR42-P-4KS2/NVR42-8P-4KS2/NVR42-16P-4KS2/NVR42-4KS2/L/NVR42-P-4KS2/L/NVR42-8P-4KS2/L/NVR42-16P-4KS2/L/NVR52-4KS2/NVR52-8P-4KS2/NVR52-16P-4KS2/ NVR52-24P-4KS2/NVR22-4KS2/NVR22-P-4KS2/NVR22-8P-4KS2/NVR52-8P-4KS2E/NVR22-I/NVR22-I2/NVR22-P-I/NVR22-P-I2/NVR22-8P-I/NVR22-8P-I2/NVR22-16P-I/NVR22-16P-I2/NVR42-I/NVR42-8P-I/NVR42-16P-I/NVR52-16P-I/NVR52-16P-I/L/NVR52-8P-I/NVR52-8P-I/L/NVR42-EI/NVR42-P-EI/NVR42-8P-EI/NVR42-16P-EI....91
3.3.4 NVR54-4KS2/NVR54-16P-4KS2/NVR44-4KS2/NVR44-16P-4KS2/NVR44-4KS2/L/NVR44-16P-4KS2/L/NVR54-24P-4KS2/NVR54-16P-4KS2E/NVR58-I/NVR58-I/L/NVR54-I/NVR54-I/L/NVR52-I/NVR52-I/L/NVR42-I/NVR42-8P-I/NVR44-I/NVR48-I/NVR608-32-4KS2/NVR44-4KS2/I/NVR44-16P-4KS2/I/NVR48-4KS2/I/NVR48-16P-4KS2/I/NVR48-EI/NVR48-16P-EI/NVR44-EI/NVR44-16P-EI....95
3.3.5 NVR608-64-4KS2/NVR608-128-4KS2/NVR608H-32-XI/NVR608H-64-XI/NVR608H-128-XI Series....99
3.3.6 NVR616-4KS2 Series....101
3.4 CD-ROM Installation....103
3.5 Connection Sample....107
3.5.1 NVR41-4KS2/NVR41-P-4KS2/NVR41-8P-4KS2/NVR41-4KS2/L/NVR41-P-4KS2/L/NVR41-8P-4KS2/L/NVR21-4KS2/NVR21-P-4KS2/NVR21-8P-4KS2/NVR21-I/NVR21-I2/

NVR21-P-I/NVR21-P-I2/NVR21-8P-I/NVR21-8P-I2/NVR21-S3/NVR21-P-S3/NVR21-8P-S3/NVR41-EI/NVR41-P-EI/NVR41-8P-EI 107
3.5.2 NVR21-W-4KS2/NVR21HS-W-4KS22 109
3.5.3 NVR11HS-S3H/NVR11HS-P-S3H/NVR11HS-8P-S3H/NVR41HS-4KS2/NVR41HS-P-4KS2/NVR41HS-8P-4KS2/NVR41HS-4KS2/L/NVR41HS-P-4KS2/L/NVR41HS-8P-4KS2/L/NVR21HS-4KS2/NVR21HS-P-4KS2/NVR21HS-8P-4KS2/NVR21HS-I/NVR21HS-I2/NVR21HS-P-I/NVR21HS-P-I2/NVR21HS-8P-I/NVR21HS-8P-I2/NVR21HS-S3/NVR21HS-P-S3/NVR21HS-8P-S3/NVR41HS-EI/NVR41HS-P-EI/NVR41HS-8P-EI 109
3.5.4 NVR22-4KS2/NVR22-P-4KS2/NVR22-8P-4KS2/NVR22-I/NVR22-I2/NVR22-P-I/NVR22-P-I2/NVR22-8P-I/NVR22-8P-I2/NVR22-16P-I/NVR22-16P-I2 Series 111
3.5.5 NVR52-4KS2/NVR52-8P-4KS2/NVR52-16P-4KS2/NVR52-24P-4KS2/NVR52-8P-4KS2E/NVR52-16P-4KS2E Series 112
3.5.6 NVR42-4KS2/NVR42-P-4KS2/NVR42-8P-4KS2/NVR42-16P-4KS2/NVR42-4KS2/L/NVR42-P-4KS2/L/NVR42-8P-4KS2/L/NVR42-16P-4KS2/L/NVR42-EI/NVR42-P-EI/NVR42-8P-EI/NVR42-16P-EI 112
3.5.7 NVR54-4KS2/NVR54-16P-4KS2/NVR58-4KS2/NVR58-16P-4KS2/NVR54-24P-4KS2/NVR54-16P-4KS2E/NVR58-16P-4KS2E Series 114
3.5.8 NVR44-4KS2/NVR44-16P-4KS2/NVR44-4KS2/L/NVR44-16P-4KS2/L/NVR44-4KS2/I/NVR44-16P-4KS2/I/NVR44-EI/NVR44-16P-EI Series 115
3.5.9 NVR48-4KS2/NVR48-16P-4KS2/NVR48-4KS2/L/NVR48-16P-4KS2/L/NVR48-4KS2/I/NVR48-16P-4KS2/I/NVR48-EI/NVR48-16P-EI Series 116
3.5.10 NVR58-I/NVR58-I/L/NVR48-I Series 117
3.5.11 NVR54-I/NVR54-I/L/NVR44-I 117
3.5.12 NVR52-16P-I/NVR52-16P-I/L/NVR52-8P-I/NVR52-8P-I/L/NVR42-8P-I/NVR42-16P-I Series 118
3.5.13 NVR4216-I Series 118
3.5.14 NVR608-4KS2/NVR608H-XI/NVR608RH-XI Series 118
3.5.15 NVR616-4KS2 Series 119
4 Starting the Device 120
5 Local Operations 121
5.1 Initialization 121
5.2 Startup Wizard 124
5.3 Login 129
5.4 Main Menu 131
5.5 Quick Operation Bar 133
5.6 Live View 135
5.6.1 Live Page 135
5.6.2 Navigation bar 135
5.6.3 Live View Control Bar 136
5.6.4 Shortcut Menu 147
5.6.5 AI Live View Mode 150
5.6.6 Split Tracking 153
5.6.7 PTZ 154

5.6.8 Wireless Pairing....166
5.6.9 Sequence....166
5.6.10 Fisheye....169
5.6.11 Temperature Monitoring....172
5.6.12 Shortcut Menu to Add Camera....173
5.6.13 Smart Tracking....174
5.7 Camera....174
5.7.1 Initializing Remote Devices....174
5.7.2 Adding Remote Devices....179
5.7.3 Changing IP Address of Remote Device....184
5.7.4 Configuring Image Settings....185
5.7.5 Configuring Overlay Settings....190
5.7.6 Configuring Encoding Settings....191
5.7.7 Modifying Channel Name....196
5.7.8 Checking the PoE Status....196
5.7.9 Updating Remote Devices....197
5.7.10 Viewing Remote Device Information....198
5.8 Recording Management....200
5.8.1 Recording Schedule....200
5.8.2 Search and Playback....207
5.8.3 Recording Information....226
5.9 AI....227
5.9.1 Overview....227
5.9.2 AI Search....228
5.9.3 Smart Plan....229
5.9.4 Face Detection....231
5.9.5 Face & Body Detection....235
5.9.6 Face Recognition....236
5.9.7 IVS....249
5.9.8 Stereo Analysis....274
5.9.9 Video Metadata....281
5.9.10 ANPR....288
5.9.11 Crowd Distribution....291
5.9.12 People Counting....293
5.9.13 Heat Map....300
5.9.14 SMD....303
5.9.15 Vehicle Density....308
5.9.16 Main-sub Tracking....310
5.9.17 Video Quality Analytics....311
5.9.18 Entries Frequency....314

5.9.19 Smart Object Detection 316
5.9.20 Smart Sound Detection 318
5.9.21 PPE Detection 319
5.10 Alarm Settings 323
5.10.1 Alarm Information 323
5.10.2 Alarm Status 324
5.10.3 Alarm Input 325
5.10.4 Alarm Output 326
5.10.5 Video Detection 327
5.10.6 Audio Detection 333
5.10.7 Thermal Alarm 333
5.10.8 Exception 334
5.10.9 Disarming 335
5.11 Network 337
5.11.1 TCP/IP 337
5.11.2 Routing Table 340
5.11.3 Port 340
5.11.4 External Wi-Fi 342
5.11.5 Wi-Fi AP 343
5.11.6 3G/4G 346
5.11.7 Cellular Network 347
5.11.8 Repeater 349
5.11.9 PPPoE 351
5.11.10 DDNS 352
5.11.11 UPnP 353
5.11.12 Email 355
5.11.13 SNMP 357
5.11.14 Multicast 359
5.11.15 Alarm Center 360
5.11.16 Register 361
5.11.17 Switch 362
5.11.18 P2P 364
5.12 Storage 365
5.12.1 Basic 365
5.12.2 Disk Manager 366
5.12.3 RAID 367
5.12.4 Disk Group 370
5.12.5 Disk Quota 371
5.12.6 Disk Check 372
5.12.7 Record Estimate 376

5.12.8 FTP....379
5.12.9 iSCSI....381
5.13 Account....382
5.13.1 Group....382
5.13.2 User....384
5.13.3 Resetting Password....387
5.13.4 ONVIF User....392
5.14 Security....394
5.14.1 Security Status....394
5.14.2 System Service....395
5.14.3 Attack Defense....399
5.14.4 CA Certificate....403
5.14.5 Audio/Video Encryption....406
5.14.6 Security Warning....408
5.15 System....409
5.15.1 General Settings....409
5.15.2 Serial Port....414
5.16 Output and Display....415
5.16.1 Display....415
5.16.2 Tour....416
5.16.3 Custom Layout....418
5.17 POS....420
5.17.1 Settings....420
5.17.2 Search....423
5.18 Audio....424
5.18.1 File Management....424
5.18.2 Audio Play....426
5.18.3 Broadcast....427
5.19 Operation and Maintenance....429
5.19.1 Log....429
5.19.2 System....430
5.19.3 Network....433
5.19.4 Maintenance and Management....436
5.20 USB Device Auto Pop-up....443
5.21 Shutdown....444
6 Web Operation....448
6.1 Network Connection....448
6.2 Web Login....448
6.3 Web Main Menu....449
6.4 Cluster Service....451

6.4.1 Configuring Cluster IP....451
6.4.2 Main Device....452
6.4.3 Sub Device....453
6.4.4 Transferring Videos....453
6.4.5 Configuring Cluster Control....453
6.4.6 Cluster Log....454
7 Glossary....456
8 FAQ....457
Appendix 1 HDD Capacity Calculation....461
Appendix 2 Mouse Operation....462
Appendix 3 Remote Control....463
Appendix 4 Compatible Network Camera List....465
Appendix 5 Cybersecurity Recommendations....471

1 Introduction

1.1 Overview

The NVR is a high performance network video recorder. This product supports local live view, multiple-window display, recorded file local storage, remote control and mouse shortcut menu operation, and remote management and control function.

This product supports center storage, front-end storage and client-end storage. The monitor zone in the front-end can be set in anywhere. Working with other front-end devices such as IPC, NVS, this series product can establish a strong surveillance network through the CMS. In the network system, there is only one network cable from the monitor center to the monitor zone in the whole network. There is no audio/video cable from the monitor center to the monitor zone. The whole project is featured by simple connection, low-cost, low maintenance work.

This NVR can be widely used in areas such as public security, water conservancy, transportation and education.

1.2 Features

AI Functions

AI functions are available on select models and vary with models.

- Face detection. The system can detect the faces are on the video image.
- Face recognition. The system can compare the detected faces with the images in the face database in real time.
- Human body detection. The system activates alarm actions once human body is detected.
- People counting. The system can effectively count the number of people and flow direction.
- Heat map. The system can monitor the active objects in a specific area.
- Automatic number plate recognition (ANPR). The system can effectively monitor the passing vehicles.

Smart Playback

This function is available on select models.

- IVS playback. It can screen out and replay the records meeting the set rules.
- Face detection playback. It can screen out and replay the records with human faces.
- Face recognition playback. It can compare the face information in the video with the information in the database and replay the corresponding records.
- ANPR playback. It can screen out the record with a specific car plate number or all the records with car plate numbers.
- Human body detection playback. It can screen out and replay the records with specific human bodies.
- Smart search. It includes smart functions such as searching by attribute and searching by image to enable users to get target records quickly.

Cloud Upgrade

For the NVR connected to the Internet, it supports application online upgrade.

Real-Time Surveillance

- VGA, HDMI port. Connect to monitor to realize real-time surveillance. Some series support TV/VGA/HDMI output at the same time.
- Shortcut menu for preview.
- Support multiple popular PTZ decoder control protocols. Support preset, tour and pattern.

Playback

- Support independent real-time recording for each channel. At the same time it supports functions such as smart search, forward play, network monitor, record search and download.
- Support various playback modes: slow play, fast play, backward play and frame-by-frame play.
- Support time title overlay so that you can view the event accurate occurred time.
- Support specified zone enlargement.

User Management

Users can be added to user groups for management. Each group has a set of permissions that can be individually edited.

Storage

- With corresponding settings (such as alarm settings and schedule settings), you can back up related audio/video data in the network video recorder.
- You can take records via the web and the record files are saved on the PC in which the client locates.

Alarm

- Respond to external alarm simultaneously (within 200 ms). Based on user's pre-defined relay settings, the system can process the alarm input correctly and sends user screen or voice prompts (supporting pre-recorded audio).
- Support settings of the central alarm server, so that the system can automatically notify users of the alarm information. Alarm input can be derived from various connected peripheral devices.
- Alert you of alarm information via email.

Network Surveillance

- Send audio/video data compressed by IPC or NVS to client-ends through the network, and then the data will be decompressed and displayed.
- Support max 128 connections at the same time.
- Transmit audio/video data by protocols such as HTTP, TCP, UDP, MULTICAST and RTP/RTCP.
- Transmit some alarm data or alarm info by SNMP.
- Support web access in WAN/LAN.

Window Split

Adopt video compression and digital processing to display several windows in one monitor. Support 1/4/8/9/16/25/36 window split in preview and 1/4/9/16 window split in playback.

Record

Support regular record, motion record, alarm record and smart record. Save the recorded files in the HDD, USB device, client-end PC or network storage server and you can search or playback the saved files at the local-end or via the Web/USB devices.

Backup

Support network backup and USB record backup. You can back up the record files in devices such as network storage server, peripheral USB 2.0 device and burner.

Network Management

- Supervise NVR configuration and control power via Ethernet.
- Support web management.

Peripheral Equipment Management

- Support peripheral device control and you can freely set the control protocol and connection port.
- Support transparent data transmission such as RS-232 and RS-485.

Auxiliary

- Support switch between NTSC and PAL.
- Support real-time display of system resources information and running status.
- Support log record.
- Local GUI output. Shortcut menu operation with the mouse.
- IR control function (for some series only). Shortcut menu operation with remote control.
- Support to play the video/audio files from remote IPC or NVS.

2 Front Panel and Rear Panel

The following front panel and rear panel figures are for reference only.

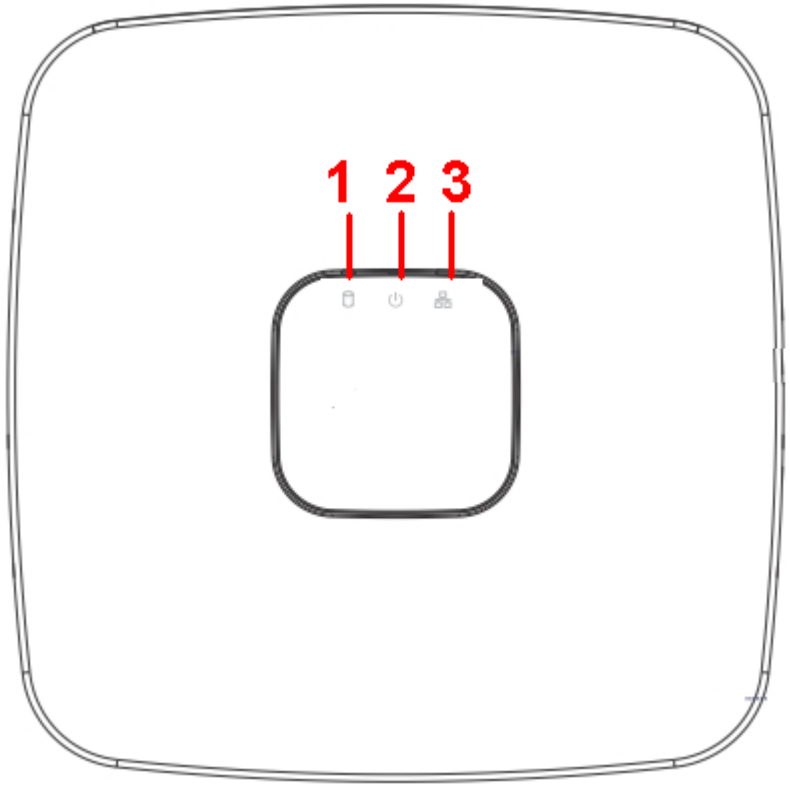
2.1 Front Panel

2.1.1 NVR41-4KS2/NVR41-P-4KS2/NVR41-8P-4KS2/ NVR41-4KS2/L/NVR41-P-4KS2/L/NVR41-8P-4KS2/L/ NVR21-4KS2/NVR21-P-4KS2/NVR21-8P-4KS2/NVR21-S3/ NVR21-P-S3/NVR21-8P-S3/NVR21-4KS3/NVR21-P-4KS3/ NVR21-8P-4KS3/NVR41-EI/NVR41-P-EI/NVR41-8P-EI/ NVR41-4KS3/NVR41-P-4KS3/NVR41-8P-4KS3 Series

The figure is for reference only.

The NVR41-4KS2/NVR41-4KS2/L/NVR41-P-4KS2/NVR41-P-4KS2/L/NVR21-4KS2/NVR21-P-4KS2/NVR21-S3/NVR21-P-S3/NVR21-4KS3/NVR21-P-4KS3/NVR41-EI/NVR41-P-EI/NVR41-4KS3/NVR41-P-4KS3 front panel is shown as below.

Figure 2-1 Front panel



The NVR41-8P-4KS2/NVR41-8P-4KS2/L/NVR21-8P-4KS2/NVR21-8P-S3/NVR41-8P-EI/NVR41-8P-4KS3/NVR21-8P-4KS3 front panel is shown as below.

Figure 2-2 Front panel

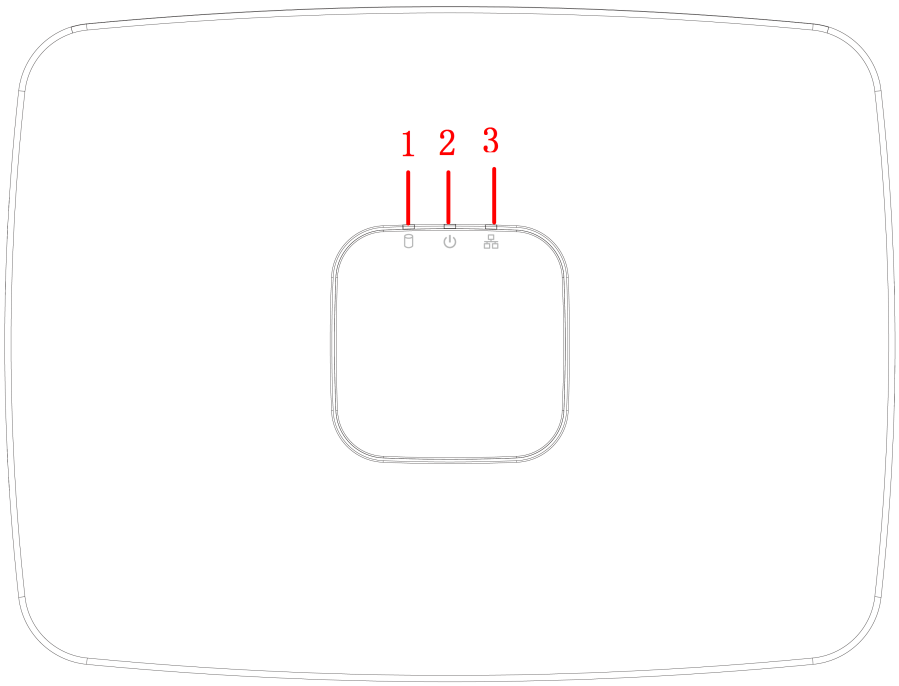


Table 2-1 Icons

No.	Name	Function
1	HDD status indicator light	The red light becomes on when HDD is abnormal.
2	Power indicator light	The red light becomes on when the power connection is normal.
3	Network status indicator light	The red light becomes on when the network connection is abnormal.

2.1.2 NVR11HS-S3H/NVR11HS-P-S3H/NVR11HS-8P-S3H/ NVR41HS-4KS2/NVR41HS-P-4KS2/NVR41HS-8P-4KS2/ NVR41HS-4KS2/L/NVR41HS-P-4KS2/L/NVR41HS-8P-4KS2/L/ NVR21HS-4KS2/NVR21HS-P-4KS2/NVR21HS-8P-4KS2/ NVR21HS-S3/NVR21HS-P-S3/NVR21HS-8P-S3/ NVR21HS-4KS3/NVR21HS-P-4KS3/NVR21HS-8P-4KS3/ NVR41HS-4KS3/NVR41HS-P-4KS3/NVR41HS-8P-4KS3

The figure is for reference only.

Figure 2-3 Front panel

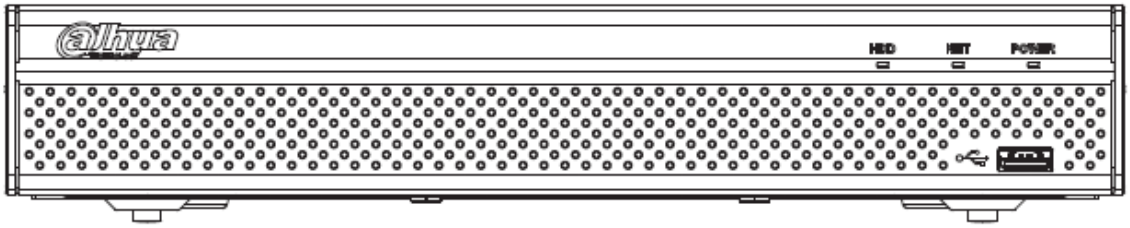


Table 2-2 Icons

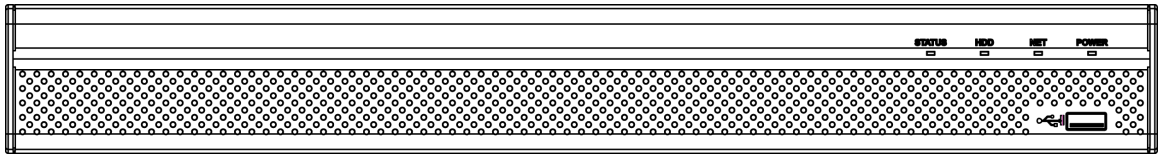
Icon	Name	Function
HDD	HDD status indicator light	The blue light is on when the HDD is malfunction.
NET	Network status indicator light	The blue light is on when the network connection is abnormal.
POWER	Power status indicator light	The blue light is on when the power connection is OK.
	USB port	Connect to peripheral USB storage device, mouse and more.

2.1.3 NVR52-4KS2/NVR52-8P-4KS2/NVR52-16P-4KS2/ NVR42-4KS2/NVR42-P-4KS2/NVR42-8P-4KS2/ NVR42-16P-4KS2/NVR42-4KS2/L/NVR42-P-4KS2/L/ NVR42-8P-4KS2/L/NVR42-16P-4KS2/L/NVR5224-24P-4KS2/ NVR54-4KS2/NVR54-16P-4KS2/NVR44-4KS2/ NVR44-16P-4KS2/NVR44-4KS2/L/NVR44-16P-4KS2/L/ NVR5424-24P-4KS2/NVR22-4KS2/NVR22-P-4KS2/ NVR22-8P-4KS2/NVR22-4KS3/NVR22-P-4KS3/ NVR22-8P-4KS3/NVR22-16P-4KS3/NVR52-8P-4KS2E/ NVR52-16P-4KS2E/NVR54-16P-4KS2E/NVR42-4KS3/NVR42-P-4KS3/NVR42-8P-4KS3/NVR44-4KS3/NVR42-16P-4KS3 Series

The figures are for reference only.

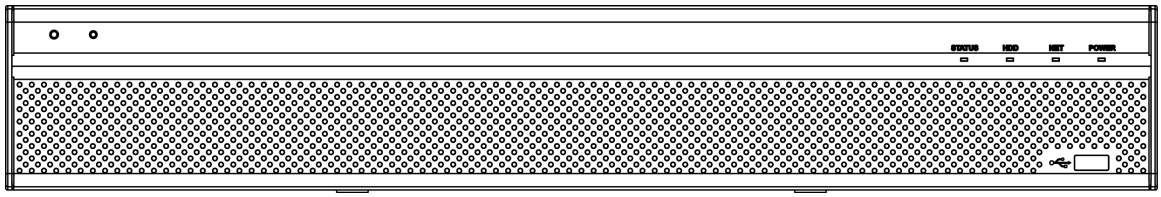
The NVR52-4KS2/NVR52-8P-4KS2/NVR52-16P-4KS2/NVR42-4KS2/NVR42-P-4KS2/NVR42-8P-4KS2/ NVR42-16P-4KS2/NVR42-4KS2/L/NVR42-P-4KS2/L/NVR42-8P-4KS2/L/NVR42-16P-4KS2/ LNVR5224-24P-4KS2/NVR22-4KS2/NVR22-P-4KS2/NVR22-8P-4KS2/NVR22-4KS3/NVR22-P-4KS3/ NVR22-8P-4KS3/NVR22-16P-4KS3/NVR52-8P-4KS2E/NVR52-16P-4KS2E/NVR42-4KS3/NVR42-P-4KS3/ NVR42-8P-4KS3/NVR42-16P-4KS3 series front panel is shown as below.

Figure 2-4 Front panel



The NVR54-4KS2/NVR54-16P-4KS2/NVR44-4KS2/NVR44-16P-4KS2/NVR44-4KS2/L/ NVR44-16P-4KS2/L/NVR54-24P-4KS2/NVR54-16P-4KS2E/NVR44-4KS3 series front panel is shown as below.

Figure 2-5 Front panel



The NVR58-4KS2/NVR58-16P-4KS2/NVR48-4KS2/NVR48-16P-4KS2/NVR48-4KS2/L/ NVR48-16P-4KS2/L/NVR58-16P-4KS2E/NVR48-4KS3 series front panel is shown as below

Figure 2-6 Front panel

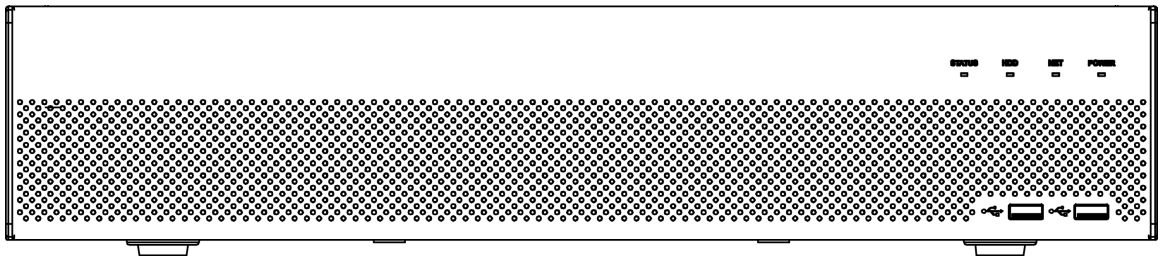


Table 2-3 Icons

Icon	Name	Function
STATUS	Status indicator light	The blue light is on when the Device is working properly.
HDD	HDD status indicator light	The blue light is on when the HDD malfunctions.
NET	Network status indicator light	The blue light is on when the network connection is abnormal.
POWER	Power status indicator light	The blue light is on when the power connection is normal.
	USB 2.0 port	Connect to peripheral USB 2.0 storage device, mouse, burner and more.

2.1.4 NVR58-4KS2/NVR58-16P-4KS2/NVR48-4KS2/ NVR48-16P-4KS2/NVR48-4KS2/L/NVR48-16P-4KS2/L/ NVR58-16P-4KS2E/NVR48-4KS3 Series

The figures are for reference only.

The NVR58-4KS2/NVR58-16P-4KS2/NVR48-4KS2/NVR48-16P-4KS2/NVR48-4KS2/L/ NVR48-16P-4KS2/L/NVR58-16P-4KS2E/NVR48-4KS3 series front panel is shown as below

Figure 2-7 Front panel

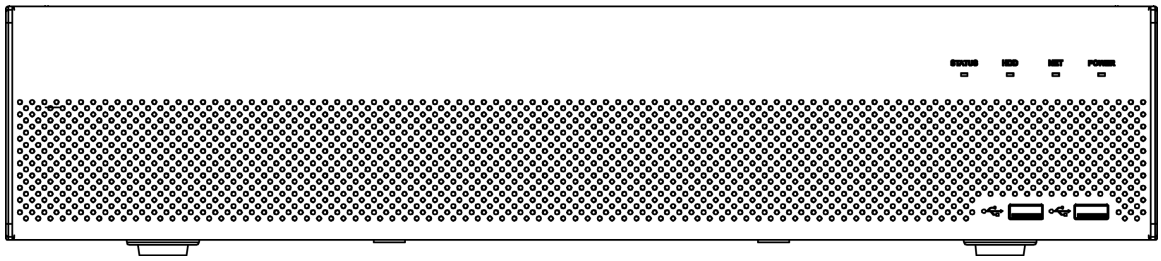


Table 2-4 Icons

Icon	Name	Function
STATUS	Status indicator light	The blue light is on when the Device is working properly.
HDD	HDD status indicator light	The blue light is on when the HDD malfunctions.
NET	Network status indicator light	The blue light is on when the network connection is abnormal.
POWER	Power status indicator light	The blue light is on when the power connection is normal.
	USB 2.0 port	Connect to peripheral USB 2.0 storage device, mouse, burner and more.

2.1.5 NVR21-W-4KS2 Series

The front panel is shown as below.

The figure is for reference only.

Figure 2-8 Front panel

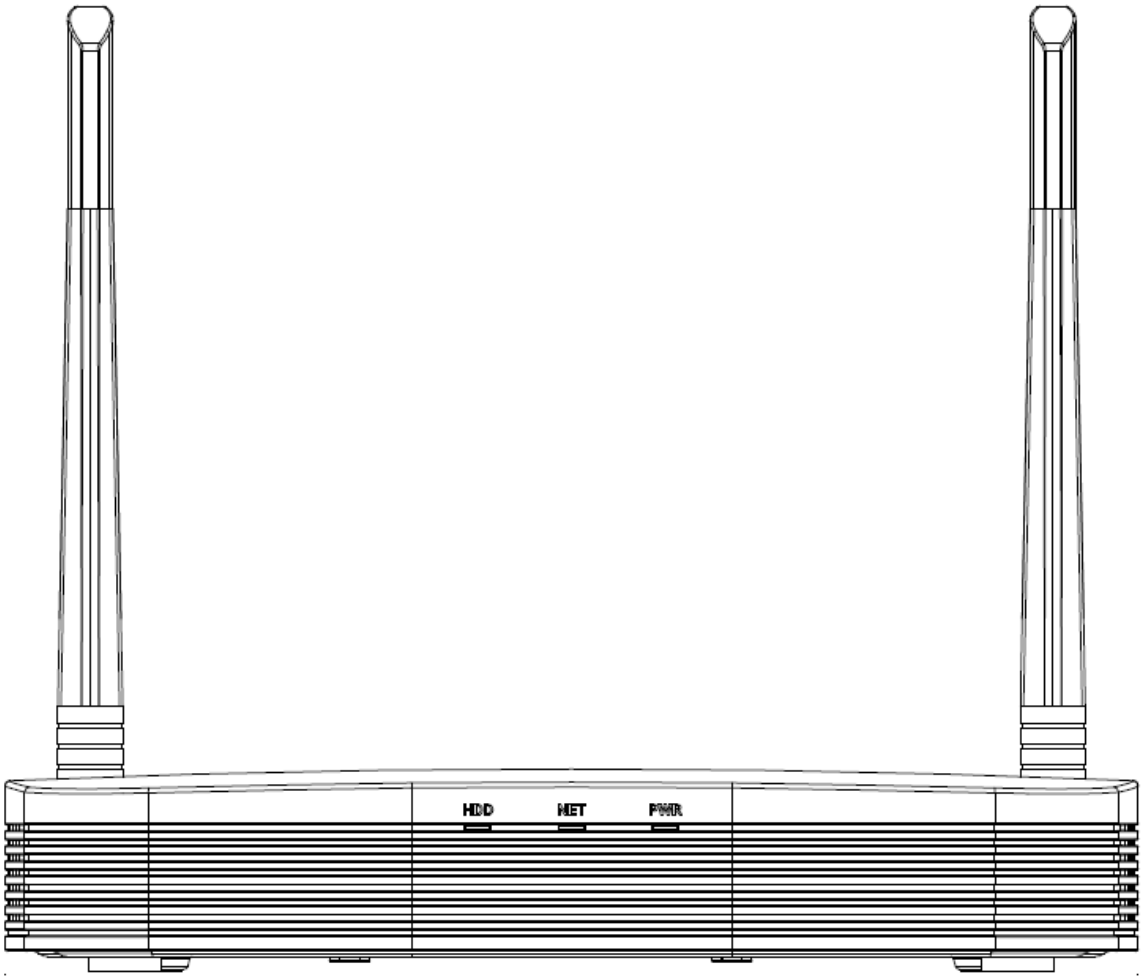


Table 2-5 Icons

Icon	Name	Function
HDD	HDD status indicator light	The blue light is on when the HDD malfunctions.
NET	Network status indicator light	The blue light is on when the network connection is abnormal.
PWR	Power status indicator light	The blue light is on when the power connection is normal.

2.1.6 NVR21HS-W-4KS2/NVR11HS-W-S2-CE/NVR11HS-W-S2-FCC Series

The front panel is shown as below.

The figure is for reference only.

Figure 2-9 Front panel

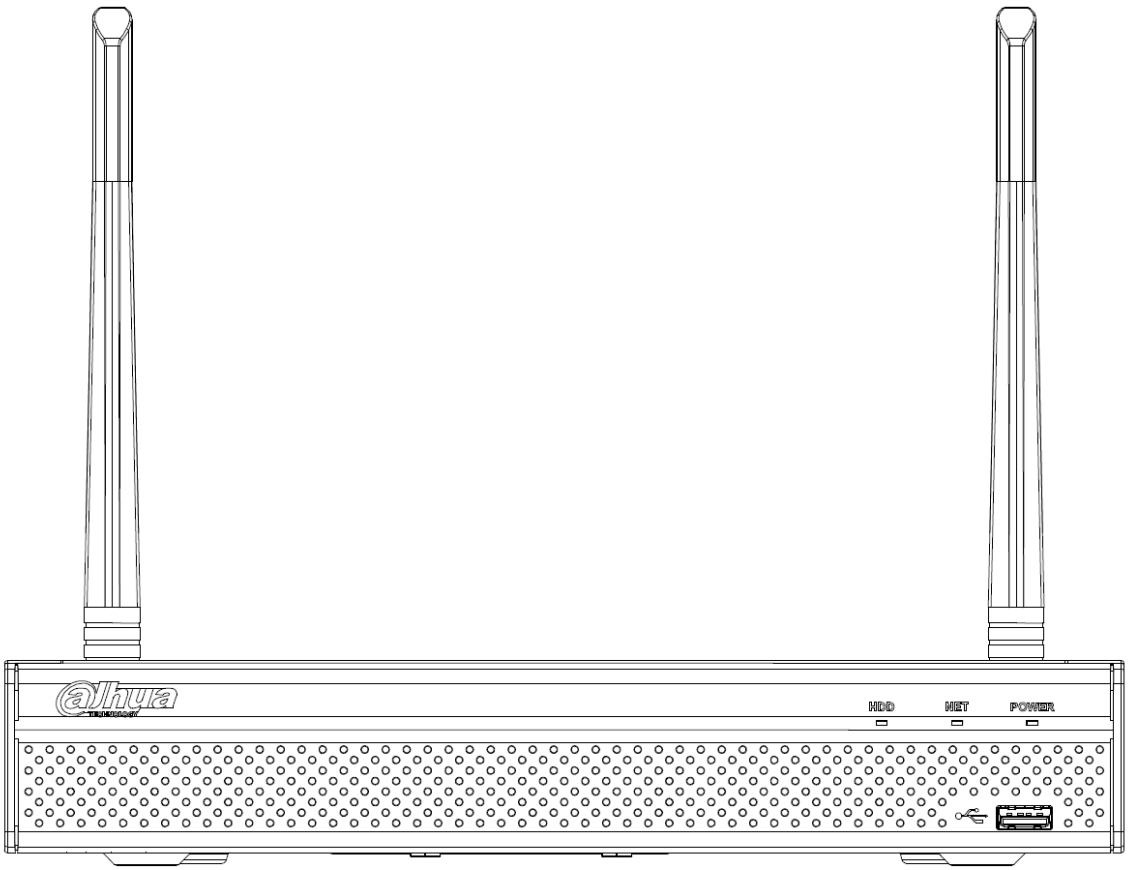


Table 2-6 Icons

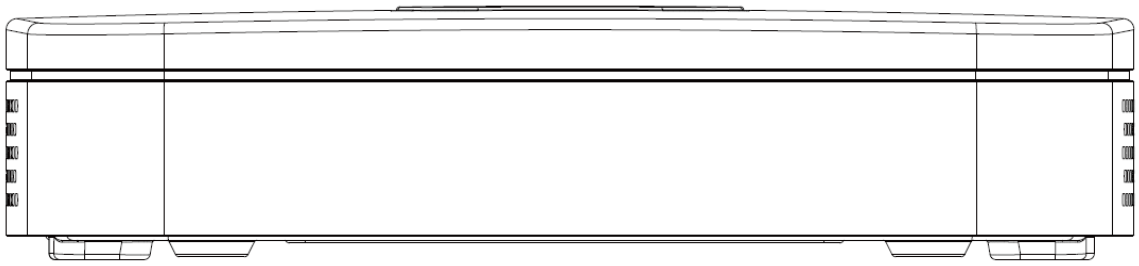
Icon	Name	Function
HDD	HDD status indicator light	The blue light is on when the HDD is malfunction.
NET	Network status indicator light	The blue light is on when the network connection is abnormal.
POWER	Power status indicator light	The blue light is on when the power connection is normal.
	USB 2.0 port	Connect to peripheral USB storage device, mouse and more.

2.1.7 NVR21-I/NVR21-I2/NVR21-P-I/NVR21-P-I2/NVR21-8P-I/NVR21-8P-I2 Series

The figure is for reference only.

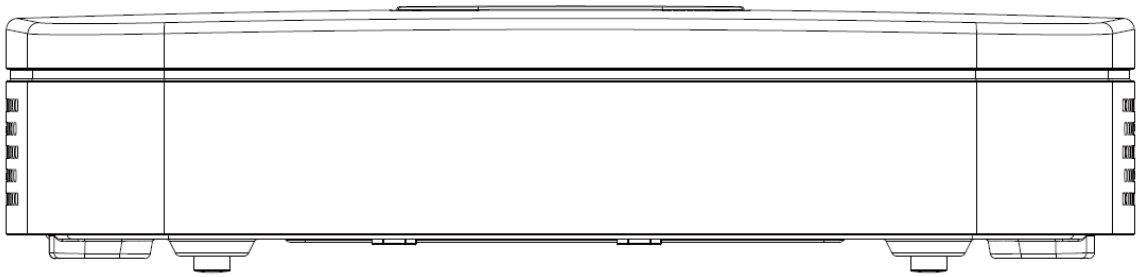
The NVR21-I/NVR21-I2 front panel is shown as below.

Figure 2-10 Front panel



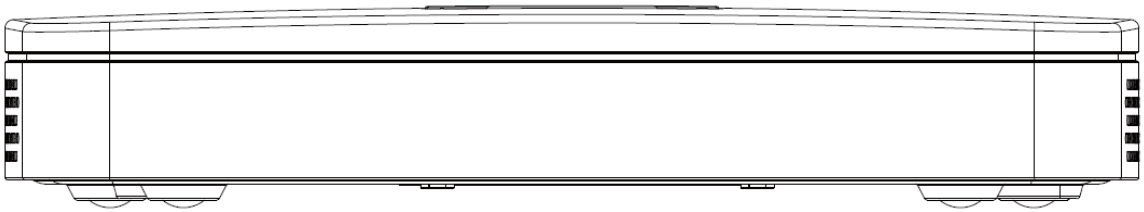
The NVR21-P-I/NVR21-P-I2 front panel is shown as below.

Figure 2-11 Front panel



The NVR21-8P-I/NVR21-8P-I2 front panel is shown as below.

Figure 2-12 Front panel



2.1.8 NVR21HS-I/NVR21HS-I2/NVR21HS-P-I/NVR21HS-P-I2/ NVR21HS-8P-I/NVR21HS-8P-I2/NVR44-4KS2/I/ NVR44-16P-4KS2/I Series

The figure is for reference only.

The NVR21HS-I/NVR21HS-I2/NVR21HS-P-I/NVR21HS-P-I2/NVR21HS-8P-I/NVR21HS-8P-I2/ NVR44-4KS2/I/NVR44-16P-4KS2/I front panel is shown as below.

Figure 2-13 Front panel

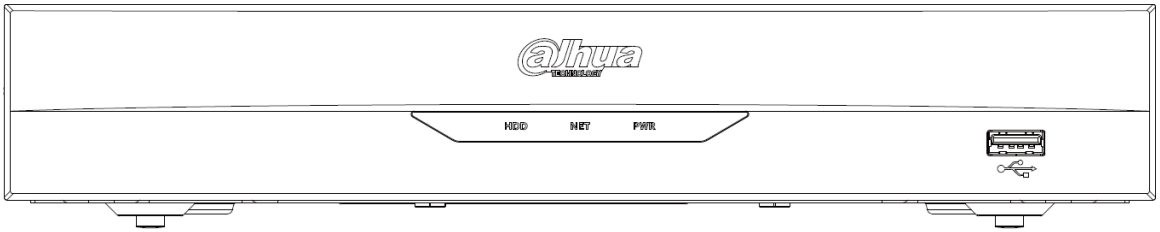


Table 2-7 Icons

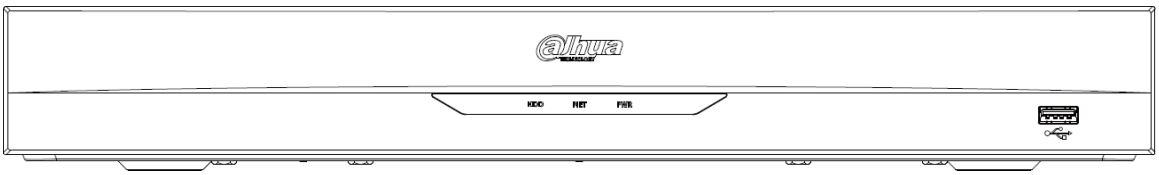
Icon	Name	Function
HDD	HDD status indicator light	The blue light is on when the HDD malfunctions.
NET	Network status indicator light	The blue light is on when the network connection is abnormal.
PWR	Power status indicator light	The blue light is on when the power connection is OK.
	USB 2.0 port	Connect to peripheral USB 2.0 storage device, mouse, burner and more.
	USB port	Connects to the external devices such as keyboard, mouse, and USB storage device.
	IR indicator	Receives signals from the remote control.

2.1.9 NVR22-I/NVR22-I2/NVR22-P-I/NVR22-P-I2/NVR22-8P-I/NVR22-8P-I2/NVR22-16P-I/NVR22-16P-I2/NVR52-EI/NVR52-8P-EI/NVR52-16P-EI/NVR41HS-EI/NVR42-EI/NVR41HS-P-EI/NVR42-P-EI/NVR41HS-8P-EI/NVR42-8P-EI/NVR42-16P-EI/NVR44-EI/NVR44-16P-EI/NVR52-XI/NVR52-8P-XI/NVR52-16P-XI/NVR54-XI/NVR58-XI

The figure is for reference only.

The NVR22-I/NVR22-I2 front panel is shown as below.

Figure 2-14 Front panel

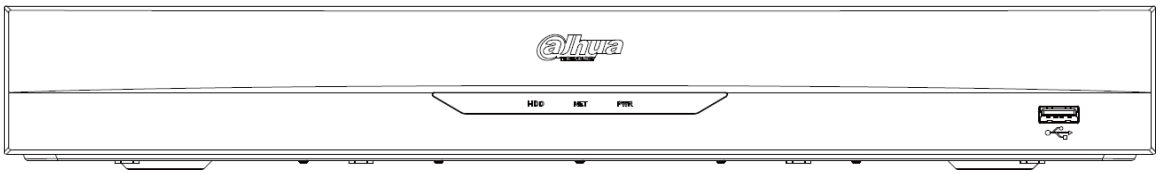


The NVR22-P-I/NVR22-P-I2 front panel is shown as below.

Figure 2-15 Front panel

The NVR22-8P-I/NVR22-8P-I2 front panel is shown as below.

Figure 2-16 Front panel

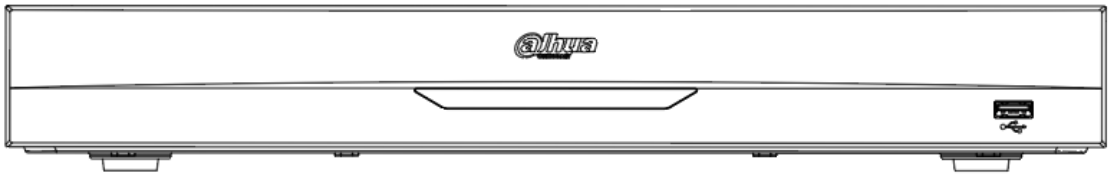


The NVR22-16P-I/NVR22-16P-I2 front panel is shown as below.

Figure 2-17 Front panel

The NVR52-EI/NVR52-8P-EI/NVR52-16P-EI/NVR54-EI/NVR54-16P-EI/NVR41HS-EI/NVR42-EI/NVR41HS-P-EI/NVR42-P-EI/NVR41HS-8P-EI/NVR42-8P-EI/NVR42-16P-EI/NVR44-EI/NVR44-16P-EI front panel is shown as below.

Figure 2-18 Front panel

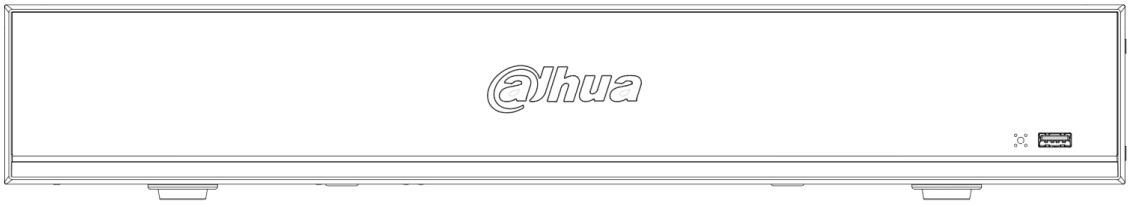


The NVR52-XI/NVR52-8P-XI/NVR52-16P-XI front panel is shown as below.

Figure 2-19 Front panel

The NVR54-XI front panel is shown as below.

Figure 2-20 Front panel



The NVR58-XI front panel is shown as below.

Figure 2-21 Front panel

Table 2-8 Icons

Icon	Name	Function
HDD	HDD status indicator light	The blue light is on when the HDD malfunctions.
NET	Network status indicator light	The blue light is on when the network connection is abnormal.
PWR	Power status indicator light	The blue light is on when the power connection is OK.
	USB 2.0 port	Connect to peripheral USB 2.0 storage device, mouse, burner and more.
	USB port	Connects to the external devices such as keyboard, mouse, and USB storage device.
	IR indicator	Receives signals from the remote control.

2.1.10 NVR48-I/NVR58-I/NVR58-I/L Series

The section takes NVR4832-I/NVR5864-I/NVR5864-I/L/NVR5832-I/NVR5832-I/L series as examples.

The figure is for reference only.

Figure 2-22 Front panel

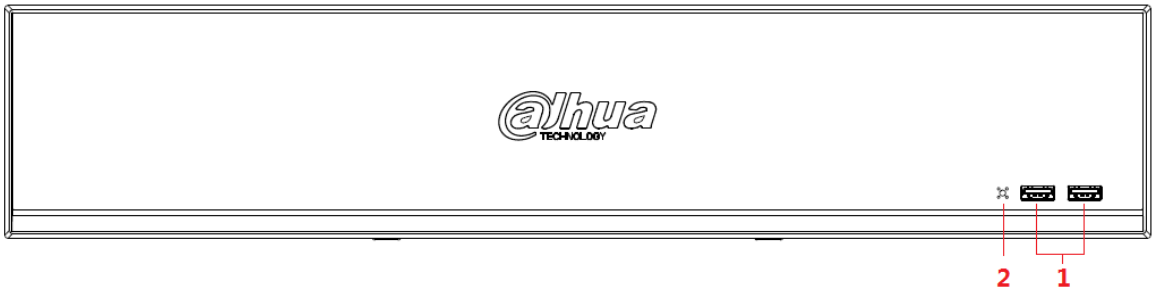


Table 2-9 Icons

No.	Port Name	Function
1	USB port	Connects to the external devices such as keyboard, mouse, and USB storage device.
2	IR indicator	Receives signals from the remote control.

2.1.11 NVR42-I/NVR44-I/NVR54-I/NVR54-I/L/NVR52-I/ NVR52-I/L Series

The section uses NVR4208-8P-I/NVR4216-I/NVR4216-16P-I/NVR4416-16P-I/NVR4432-I/ NVR5432-16P-I/NVR5432-16P-I/L/ NVR5216-16P-I/NVR5216-16P-I/L/NVR5216-8P-I/NVR5216-8P-I/L series as examples.

The figure is for reference only.

Figure 2-23 Front panel

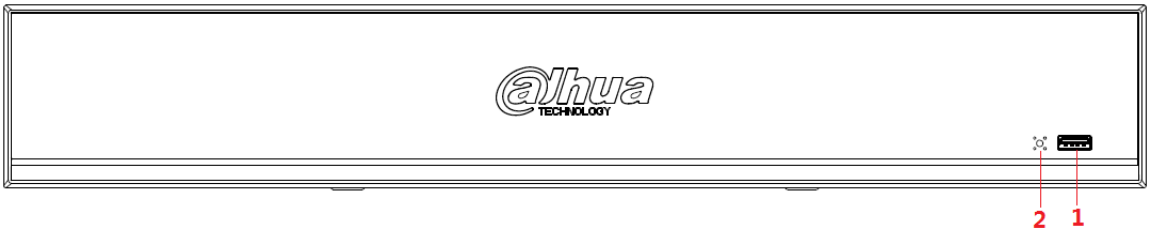


Table 2-10 Icons

No.	Port Name	Function
1	USB port	Connects to the external devices such as keyboard, mouse, and USB storage device.
2	IR indicator	Receives signals from the remote control.

2.1.12 NVR48-4KS2/I/NVR48-16P-4KS2/I/NVR54-EI/ NVR54-16P-EI/NVR58-EI/NVR58-16P-EI/NVR48-EI/ NVR48-16P-EI

The figures are for reference only.

The NVR48-4KS2/I/NVR48-16P-4KS2/I series front panel is shown as below.

Figure 2-24 Front panel

The NVR54-EI / NVR54-16P-EI front panel is shown as below.

Figure 2-25 Front panel

The NVR58-EI/NVR58-16P-EI/NVR48-EI/NVR48-16P-EI front panel is shown as below.

Figure 2-26 Front panel

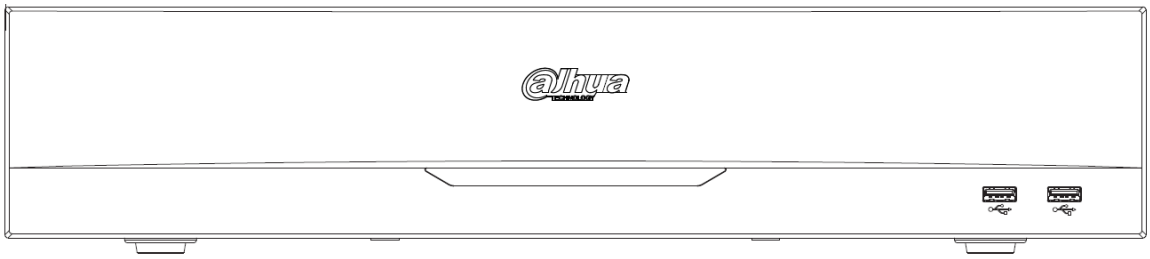


Table 2-11 Icons

Icon	Name	Function
HDD	HDD status indicator light	The blue light is on when the HDD malfunctions.
NET	Network status indicator light	The blue light is on when the network connection is abnormal.
PWR	Power status indicator light	The blue light is on when the power connection is normal.
	USB 2.0 port	Connect to peripheral USB 2.0 storage device, mouse, burner and more.

2.1.13 NVR608-32-4KS2 Series

The following figures are for reference only.

The NVR608-32-4KS2 front panel is shown as below.

Figure 2-27 Front panel

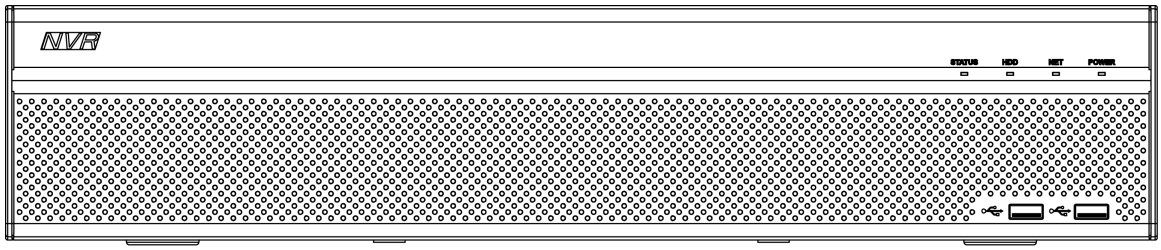


Table 2-12 Icons description

Icon	Name	Function
STATUS	Status indicator light	The blue light is on when the device is working properly.
HDD	HDD status indicator light	The blue light is on when the HDD malfunctions.
NET	Network status indicator light	The blue light is on when the network connection is abnormal.
POWER	Power status indicator light	The blue light is on when the power connection is normal.
	USB 2.0 port	Connect to peripheral USB 2.0 storage device, mouse, burner and more.

2.1.14 NVR608-64-4KS2/NVR608-128-4KS2/NVR608H-XI/ NVR608RH-XI Series

The NVR608-64-4KS2/NVR608-128-4KS2/NVR608H-32-XI/NVR608H-64-XI/NVR608H-128-XI/ NVR608RH-32-XI/NVR608RH-64-XI/NVR608RH-128-XI front panel is shown as below.

Figure 2-28 Front panel

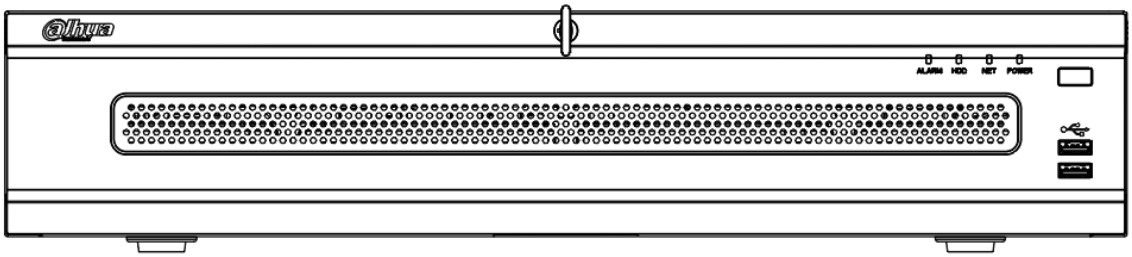


Table 2-13 Front panel description

Icon	Name
ALARM	Alarm indicator light
HDD	HDD status indicator light

Icon	Name
NET	Network status indicator light
POWER	Power status indicator light
	USB 2.0 port
	Power on-off button

2.1.15 NVR616-4KS2/NVR616-XI/NVR50-EI Series

The following figures are for reference only.

For the product of LCD, the front panel of NVR616-4KS2/NVR616-XI series is shown as below.

Figure 2-29 Front panel

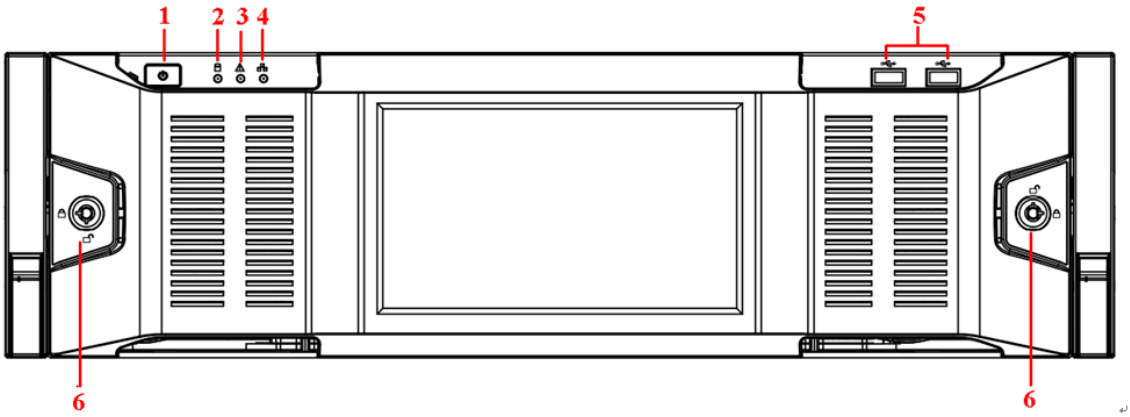


Table 2-14 Icons

No.	Name	Function
1	Power button	Press it once to turn on the device. Press it for a long time to turn off the device. ● We do not recommend you turn off the device in this way. ● Press power button for a long time or pull out the power cable might result in device auto restart.
2	System HDD indicator light	The blue light becomes on after system booted up properly. In the system HDD, there are device important configuration file, factory default configuration file, and device initial boot up data.

No.	Name	Function
3	Alarm indicator light	The alarm indicator light becomes on once an alarm occurred. It becomes on via the software detection. The indicator light becomes on when there is a local alarm.
4	Network indicator light	The blue network indicator light is on after you connected the device to the network.
5	USB port	—
6	Front panel lock	—

For general NVR616-4KS2/NVR616-XI/NVR50-EI series, the front panel is shown as below.

Figure 2-30 Front panel

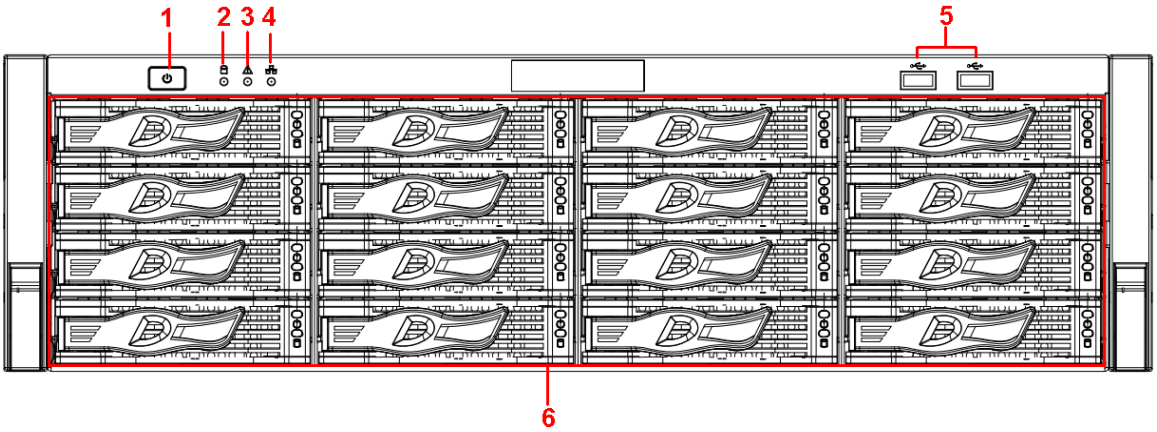


Table 2-15 Icons

No.	Name	Function
1	Power button	Press it once to turn on the device. Press it for a long time to turn off the device. ● We do not recommend you turn off the device in this way. ● Press power button for a long time or pull out the power cable might result in device auto restart.
2	System HDD Indicator light	The blue light becomes on after system booted up properly. In the system HDD, there are device important configuration file, factory default configuration file, device initial boot up data.
3	Alarm indicator light	The alarm indicator light becomes on once an alarm occurred. It becomes on via the software detection. The indicator light becomes on when there is a local alarm.
4	Network indicator light	The blue network indicator light is on after you connected the device to the network.

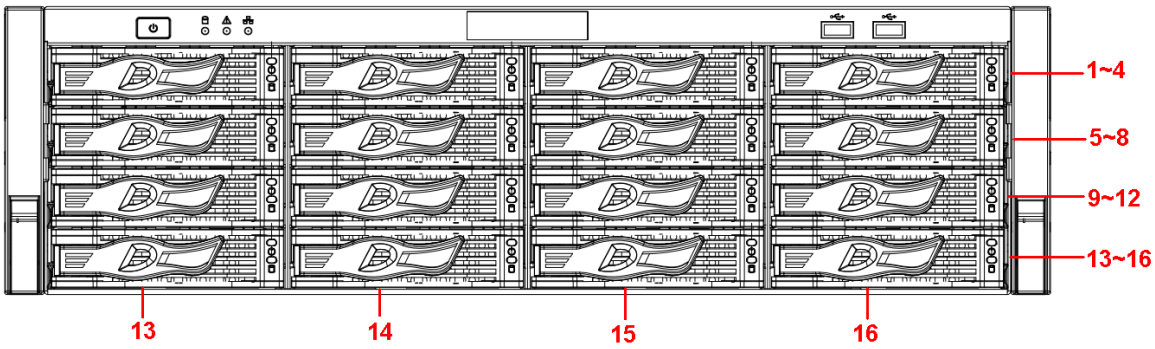
5	USB port	—
6	16 HDD slot	—

After you remove the front panel, you can see there are 16 HDDs. From the left to the right and from the top to the bottom, it ranges from 1-4, 5-8, 9-12, 13-16.

You can see there are two indicator lights on the HDD bracket.

- The power indicator light is at the top. The light is yellow after you connected the device to the power.
- The read-write indicator light is at the bottom. The blue light flashes when system is reading or writing the data. In addition to flashing blue light, read-write operation lights of some models of devices further include the following states. Please refer to the actual device.
  - Stead red: HDD failure (HDD error).
  - Flash red: HDD is in a RAID rebuild state.
  - Red intermittent flashing twice: HDD is in a predicted fault state (including a HDD warning).
  - Blue and red flashing alternately: HDD is in a positioned state.

Figure 2-31 Front panel



2.1.16 NVR624-XI Series

The following figures are for reference only.

The front panel of NVR624-XI series is shown as follows.

Figure 2-32 Front panel

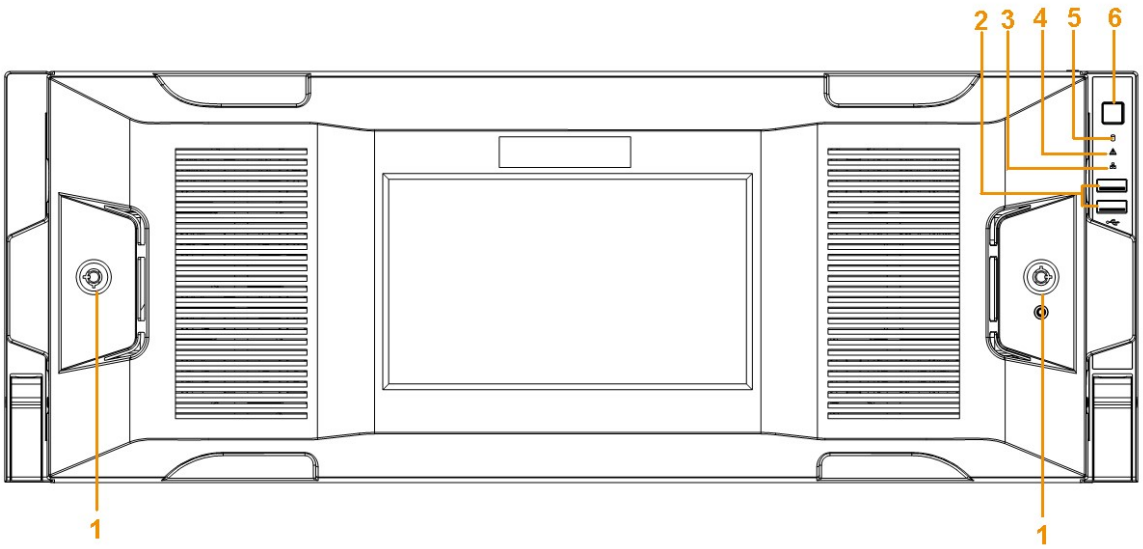


Table 2-16 Icons

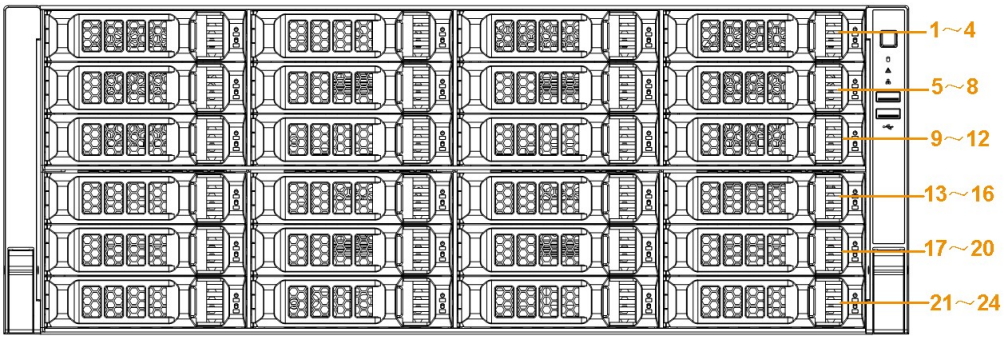
No.	Name	Function
1	Front panel lock	—
2	USB port	—
3	Network indicator light	The blue network indicator light is on after you connected the device to the network.
4	Alarm indicator light	The alarm indicator light becomes on once an alarm occurred. It becomes on via the software detection. The indicator light becomes on when there is a local alarm.
5	System HDD indicator light	The blue light becomes on after system booted up properly. In the system HDD, there are device important configuration file, factory default configuration file, and device initial boot up data.
6	Power button	Press it once to turn on the device. Press it for a long time to turn off the device. ● We do not recommend you turn off the device in this way. ● Press power button for a long time or pull out the power cable might result in device auto restart.

You can see there are 24 HDDs. From the left to the right and from the top to the bottom, it ranges from 1-4, 5-8, 9-12, 13-16, 17-20, 21-24.

You can see there are two indicator lights on the HDD bracket.

- The power indicator light is at the top. The light is yellow after you connected the device to the power.
- The read-write indicator light is at the bottom. The blue light flashes when system is reading or writing the data. In addition to flashing blue light, read-write operation lights of some models of devices further include the following states. Please refer to the actual device.
  - ◇ Stead red: HDD failure (HDD error).
  - ◇ Flash red: HDD is in a RAID rebuild state.
  - ◇ Red intermittent flashing twice: HDD is in a predicted fault state (including a HDD warning).
  - ◇ Blue and red flashing alternately: HDD is in a positioned state.

Figure 2-33 Front panel

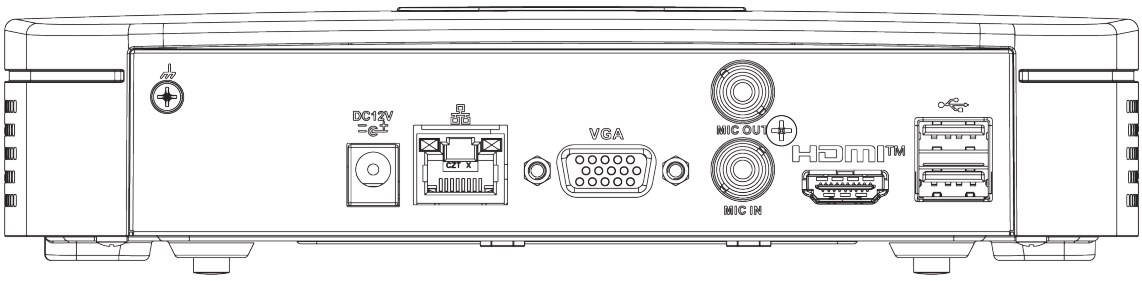


2.2 Rear Panel

2.2.1 NVR21-4KS2/NVR21-P-4KS2/NVR21-8P-4KS2/ NVR21-4KS3/NVR21-P-4KS3/NVR21-8P-4KS3/NVR41-EI/ NVR41-8P-EI/NVR41-P-EI/NVR41-4KS3/NVR41-P-4KS3/ NVR41-8P-4KS3 Series

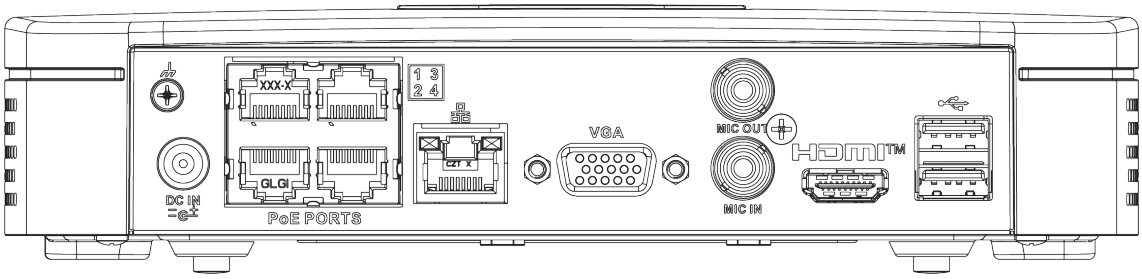
The NVR21-4KS2/NVR21-4KS3/NVR41-EI//NVR41-4KS3 is shown as below.

Figure 2-34 Rear panel



The NVR41-P-EI/NVR21-P-4KS2/NVR21-P-4KS3/NVR41-P-4KS3 is shown as below.

Figure 2-35 Rear panel



The NVR21-8P-4KS2/NVR21-8P-4KS3/NVR41-8P-EI/NVR41-8P-4KS3 is shown as below.

Figure 2-36 Rear panel

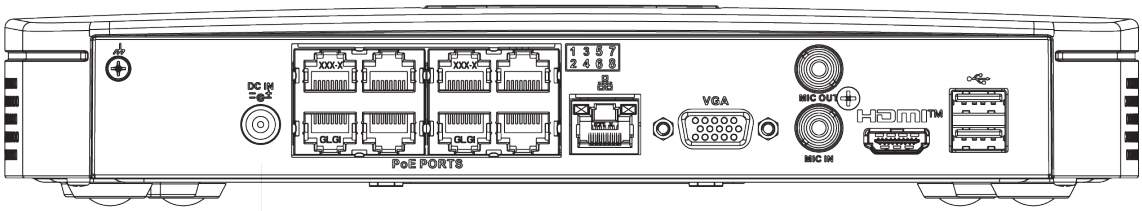


Table 2-17 Ports

Port Name	Connection	Function
DC 12V / DC IN	Power input port	Power socket. ● For NVR21-S2/21-4KS2/NVR21-4KS3/NVR41-EI/NVR41-4KS3, input 12 VDC/2 A. ● For NVR21-P-S2/21-P-4KS2, input 48 VDC/1.25 A. ● For NVR21-8P-S2/21-8P-4KS2, input 48 VDC/2 A. ● For NVR21-4KS3, input 12 VDC/1.5 A. ● For NVR21-P-4KS3, input 53 VDC/1.22 A. ● For NVR21-8P-4KS3, input 53 VDC/1.81 A. ● For NVR41-P-EI/NVR41-P-4KS3 series, input 53 VDC/1.22 A. ● For NVR41-8P-EI/NVR41-8P-4KS3 series, input 53 VDC/1.81 A.

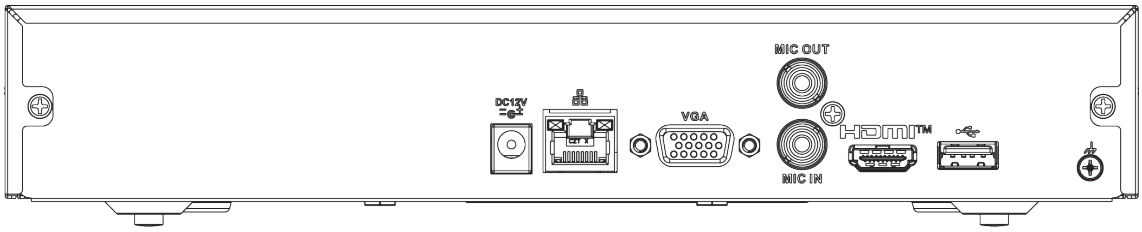
Port Name	Connection	Function
	Network port	10/100/1000 Mbps self-adaptive Ethernet port. Connect to the network cable. ● NVR41-EI/NVR41-4KS3 series supports 10/100 Mbps or 10/100/1000 Mbps. ● NVR41-P-EI/NVR41-P-4KS3 series supports 10/100 Mbps. ● NVR41-8P-EI/NVR41-8P-4KS3 series supports 10/100/1000 Mbps. The parameters might be different according to the models. Please refer to actual device for detailed information.
	USB port	USB port. Connect to mouse, USB storage device and more.
HDMI	High Definition Media Page	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
VGA	VGA video output port	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video.
MIC IN	Audio input port	Bidirectional talk input port. It is to receive the analog audio signal output from the devices such as microphone, pickup.
MIC OUT	Audio output port	Audio output port. It is to output the analog audio signal to the devices such as the sound box. ● Bidirectional talk output. ● Audio output on 1-window video monitor. ● Audio output on 1-window video playback.
	GND	Ground end.
PoE PORTS	PoE port	Built-in switch. Support PoE function. For PoE series product, you can use this port to provide power to the network camera.

2.2.2 NVR11HS-S3H/NVR11HS-P-S3H/NVR11HS-8P-S3H/ NVR21HS-4KS2/NVR21HS-P-4KS2/NVR21HS-8P-4KS2/ NVR41HS-4KS2/NVR41HS-P-4KS2/NVR41HS-8P-4KS2/ NVR41HS-4KS2/L/NVR41HS-P-4KS2/L/NVR41HS-8P-4KS2/L/ NVR21HS-S3/NVR21HS-P-S3/NVR21HS-8P-S3/ NVR21HS-4KS3/NVR21HS-P-4KS3/NVR21HS-8P-4KS3/

NVR41HS-EI/NVR41HS-P-EI/NVR41HS-8P-EI/NVR41HS-4KS3/NVR41HS-P-4KS3/NVR41HS-8P-4KS3

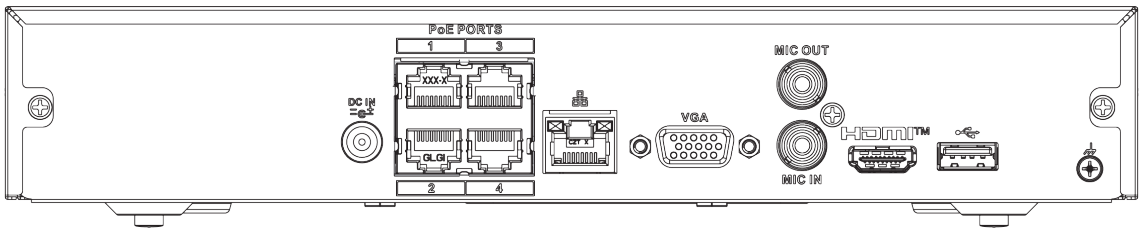
The NVR11HS-S3H/NVR21HS-4KS2/NVR41HS-4KS2/NVR41HS-4KS2/L/NVR21HS-S3/NVR21HS-4KS3/NVR41HS-EI/NVR41HS-4KS3 series rear panel is shown as below.

Figure 2-37 Rear panel



The NVR11HS-P-S3H/NVR21HS-P-4KS2/NVR41HS-P-4KS2/NVR41HS-P-4KS2/L/NVR21HS-P-S3/NVR21HS-P-4KS3/NVR41HS-P-EI/NVR41HS-P-4KS3 series rear panel is shown as below.

Figure 2-38 Rear panel



The NVR11HS-8P-S3H/NVR21HS-8P-4KS2/NVR41HS-8P-4KS2/NVR41HS-8P-4KS2/L/NVR21HS-8P-S3/NVR21HS-8P-4KS3/NVR41HS-8P-EI/NVR41HS-8P-4KS3 series rear panel is shown as below.

Figure 2-39 Rear panel

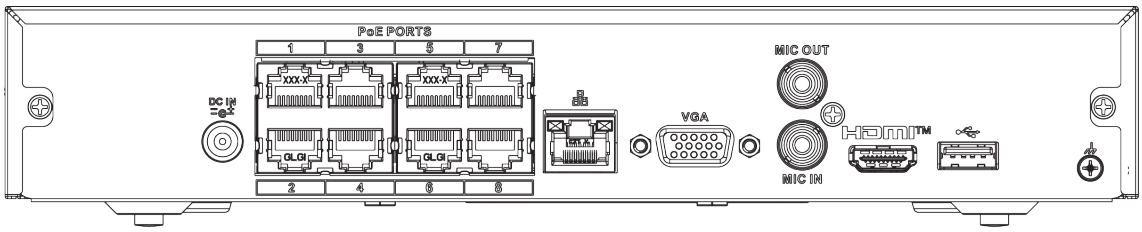


Table 2-18 Ports

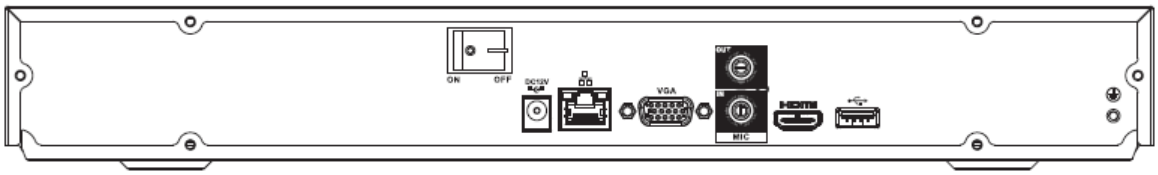
Port Name	Connection	Function
DC 12V / DC IN	Power input port	Power socket. ● For NVR11HS-P-S3H/NVR21HS-4KS2/NVR41HS-4KS2/ NVR41HS-EI/NVR41HS-4KS3 series, input 12 VDC/2 A. ● For NVR11HS-P-S3H/NVR21HS-P-4KS2/ NVR41HS-4KS2 series, input 48 VDC/1.25 A. ● For NVR11HS-8P-4KS2/NVR21HS-8P-4KS2/ NVR41HS-4KS2 series, input 48 VDC/2 A. ● For NVR21HS-4KS3, input 12 VDC/1.5 A. ● For NVR21HS-P-4KS3, input 53 VDC/1.22 A. ● For NVR21HS-8P-4KS3, input 53 VDC/1.81 A. ● For NVR41HS-P-EI/NVR41HS-P-4KS3 series, input 53 VDC/1.22 A. ● For NVR41HS-8P-EI/NVR41HS-8P-4KS3 series, input 53 VDC/1.81 A.
	Network port	10/100/1000 Mbps self-adaptive Ethernet port. Connect to the network cable. ● NVR41HS-EI/NVR41HS-4KS3 series supports 10/100 Mbps or 10/100/1000 Mbps. ● NVR41HS-P-EI/NVR41HS-P-4KS3 series supports 10/100 Mbps. ● NVR41HS-8P-EI/NVR41HS-8P-4KS3 series supports 10/100/1000 Mbps. The parameters might be different according to the models. Please refer to actual device for detailed information.
	USB port	USB port. Connect to mouse, USB storage device and more.
HDMI	High Definition Media Page	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
VGA	VGA video output port	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video.
MIC IN	Audio input port	Bidirectional talk input port. It is to receive the analog audio signal output from the devices such as microphone, pickup.
MIC OUT	Audio output port	Audio output port. It is to output the analog audio signal to the devices such as the sound box. ● Bidirectional talk output. ● Audio output on 1-window video monitor. ● Audio output on 1-window video playback.

Port Name	Connection	Function
⏚	GND	Ground end.
PoE PORTS	PoE port	Built-in switch. Support PoE function. For PoE series product, you can use this port to provide power to the network camera.

2.2.3 NVR22-4KS2/NVR22-P-4KS2/NVR22-8P-4KS2// NVR22-4KS3/NVR22-P-4KS3/NVR22-8P-4KS3/ NVR22-16P-4KS3 Series

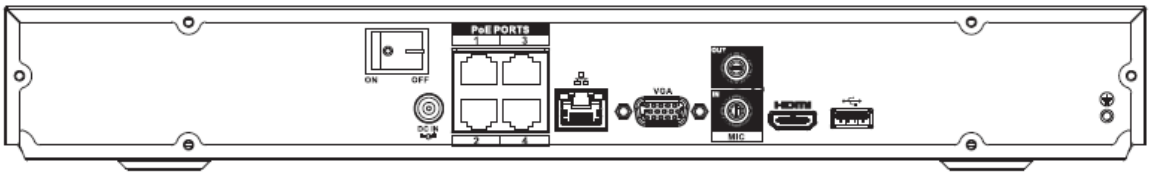
The NVR22-4KS2 series rear panel is shown as below.

Figure 2-40 Rear panel



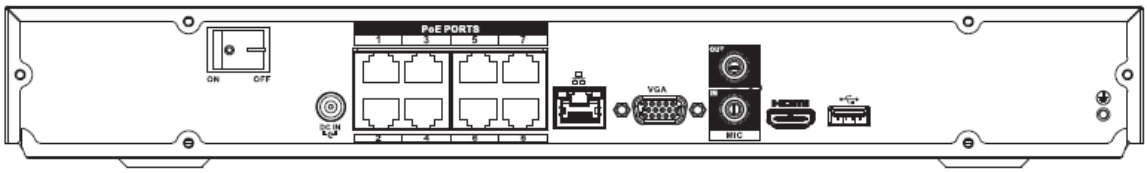
The NVR22-P-4KS2 series rear panel is shown as below.

Figure 2-41 Rear panel



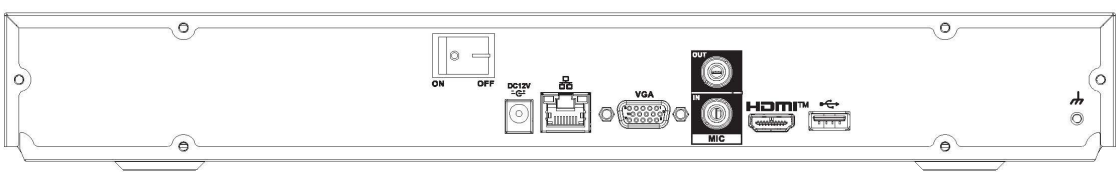
The NVR22-8P-4KS2 series rear panel is shown as below.

Figure 2-42 Rear panel



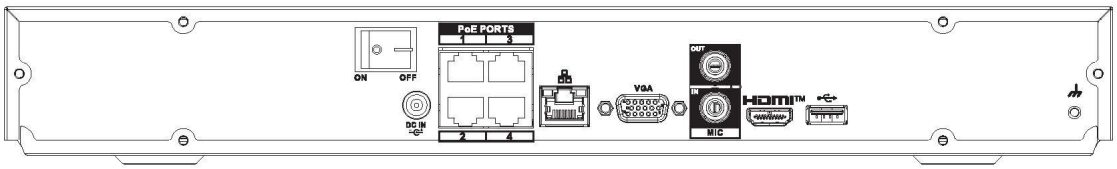
The NVR22-4KS3 series rear panel is shown as below.

Figure 2-43 Rear panel



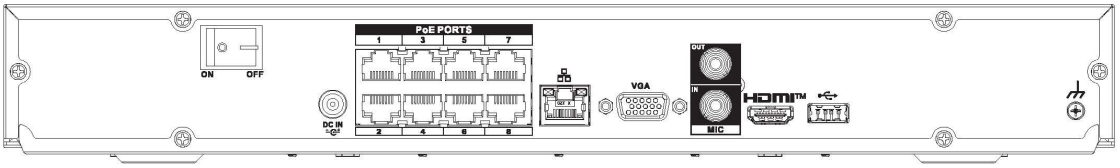
The NVR22-P-4KS3 series rear panel is shown as below.

Figure 2-44 Rear panel



The NVR22-8P-4KS3 series rear panel is shown as below.

Figure 2-45 Rear panel



The NVR22-16P-4KS3 series rear panel is shown as below.

Figure 2-46 Rear panel

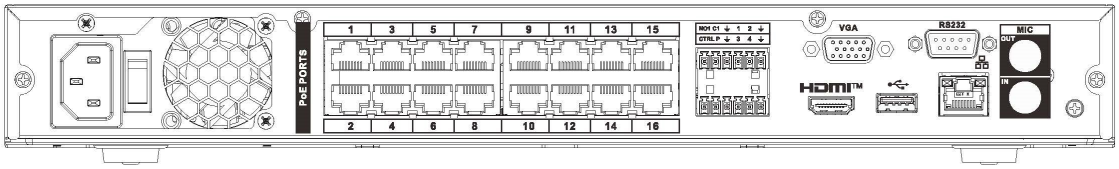


Table 2-19 Rear panel description

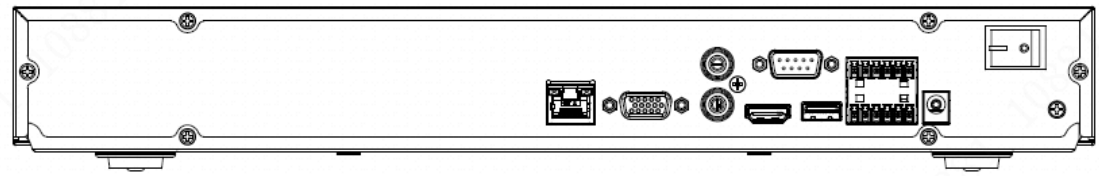
Port Name	Connection	Function
DC 12V / DC IN	Power input port	Power socket. ● For NVR22-4KS2general series, input 12 VDC/4 A. ● For NVR22-P-4KS2 series, input 48 VDC/1.5 A. ● For NVR22-8P-4KS2 series, input 53 VDC 120 W. ● For NVR22-P-4KS3, input 53 VDC/1.81 A. ● For NVR22-8P-4KS3, input 54 VDC/2.22 A.
	Network port	10/100 Mbps self-adaptive Ethernet port. Connect to the network cable.
	USB port	USB port. Connect to mouse, USB storage device and more.
HDMI	High Definition Media Page	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
VGA	VGA video output port	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video.
MIC IN	Audio input port	Bidirectional talk input port. It is to receive the analog audio signal output from the devices such as microphone, pickup.

Port Name	Connection	Function
MIC OUT	Audio output port	Audio output port. It is to output the analog audio signal to the devices such as the sound box. ● Bidirectional talk output. ● Audio output on 1-window video monitor. ● Audio output on 1-window video playback.
⏚	GND	Ground end.
PoE PORTS	PoE port	Built-in switch. Support PoE function. For PoE series product, you can use this port to provide power to the network camera.

2.2.4 NVR52-4KS2/NVR52-8P-4KS2/NVR52-16P-4KS2/ NVR52-24P-4KS2/NVR52-8P-4KS2E/NVR52-16P-4KS2E/ NVR52-EI/NVR52-8P-EI/NVR52-16P-EI/NVR42-16P-EI Series

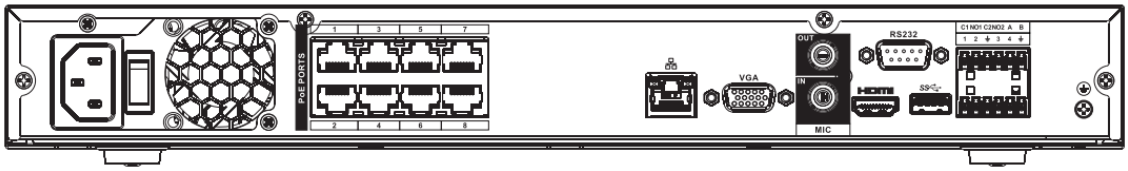
The NVR52-4KS2 series rear panel is shown as below.

Figure 2-47 Rear panel



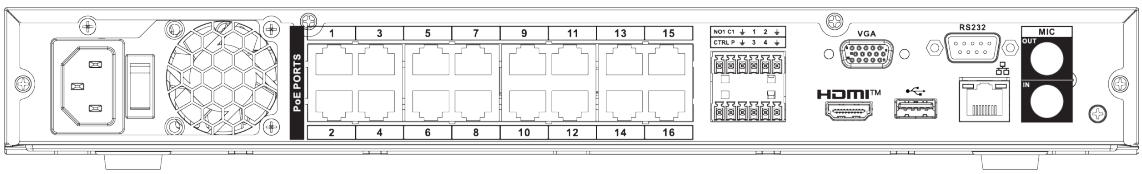
The NVR52-8P-4KS2 series rear panel is shown as below.

Figure 2-48 Rear panel



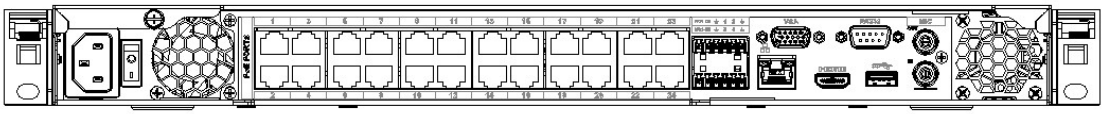
The NVR52-16P-4KS2/NVR42-16P-EI series rear panel is shown as below.

Figure 2-49 Rear panel



The NVR52-24P-4KS2 series rear panel is shown as below.

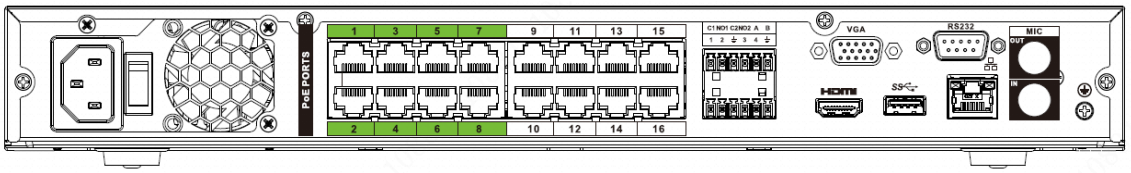
Figure 2-50 Rear panel



The NVR52-8P-4KS2E/52-16P-4KS2E series rear panel is shown as below.

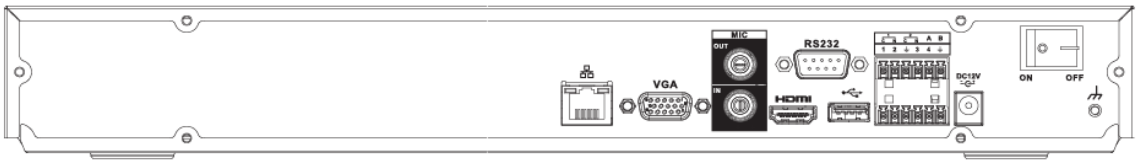
The following figure takes NVR52-16P-4KS2E series as an example. NVR52-8P-4KS2E has 8 PoE ports only.

Figure 2-51 Rear panel



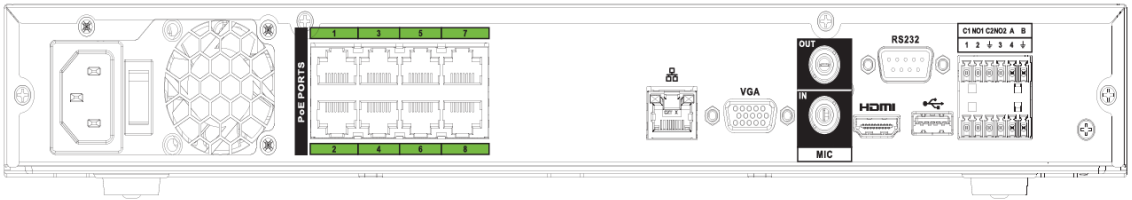
The NVR52-EI series rear panel is shown as below.

Figure 2-52 Rear panel



The NVR52-8P-EI series rear panel is shown as below.

Figure 2-53 Rear panel



The NVR52-16P-EI series rear panel is shown as below.

Figure 2-54 Rear panel

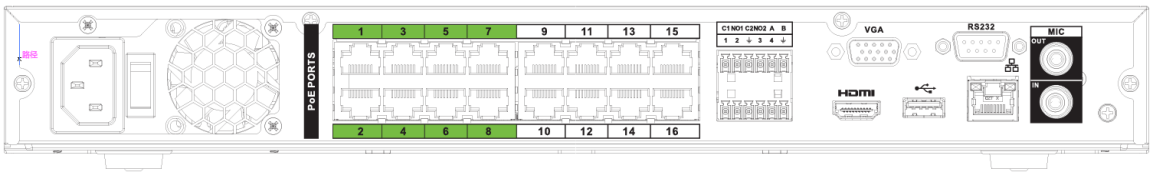


Table 2-20 Ports

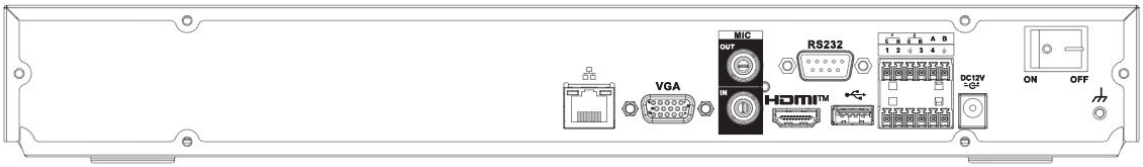
Icon	Port Name	Function
	Network port	10/100/1000 Mbps self-adaptive Ethernet port. Connect to the network cable.
HDMI	High Definition Media Page	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
SS	USB port	Connect to mouse, USB storage device, USB burner and more.
RS-232	RS-232 debug COM	It is for general COM debug to configure IP address or transfer transparent COM data.
VGA	VGA video output port	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video.
MIC IN	Audio input port	Bidirectional talk input port. It is to receive the analog audio signal output from the devices such as microphone, pickup.
MIC OUT	Audio output port	Audio output port. It is to output the analog audio signal to the devices such as the sound box. ● Bidirectional talk output. ● Audio output on 1-window video monitor. ● Audio output on 1-window video playback.
1–8	Alarm input port 1–8	● There are two groups. The first group is from port 1 to port 4; the second group is from port 5 to port 8. They are to receive the signal from the external alarm source. There are two types; NO (normal open)/NC (normal close). ● When your alarm input device is using external power, please make sure the device and the NVR have the same ground.
⏚	GND	Alarm input ground port.
NO1–NO3	Alarm output port 1–3	● 3 groups of alarm output ports. (Group 1: port NO1–C1; Group 2: port NO2–C2; Group 3: port NO3–C3). Output alarm signal to the alarm device. Please make sure there is power to the external alarm device. ● NO: Normal open alarm output port. ● C: Alarm output public end.
C1–C3		
A	RS-485 communication port	RS485_A port. It is the cable A. You can connect to the control devices such as speed dome PTZ.
B		RS485_B. It is the cable B. You can connect to the control devices such as speed dome PTZ.
DC 12V	Power input port	Input 12 VDC/4 A.
Power Switch	—	Power on/off button.

Icon	Port Name	Function
PoE PORTS	—	Built-in Switch. Support PoE or ePoE function. ● For ePoE series product, port 1 to port 8 are the ePoE ports. ePoE port supports 300 meters@100 Mbps, 800 meters@10 Mbps. Port 9 to port 16 are general PoE ports. ● The 8 PoE series product supports total 130 W. ● The 16 PoE series product supports total 130 W.

2.2.5 NVR52-XI/NVR52-8P-XI/NVR-52-16P-XI Series

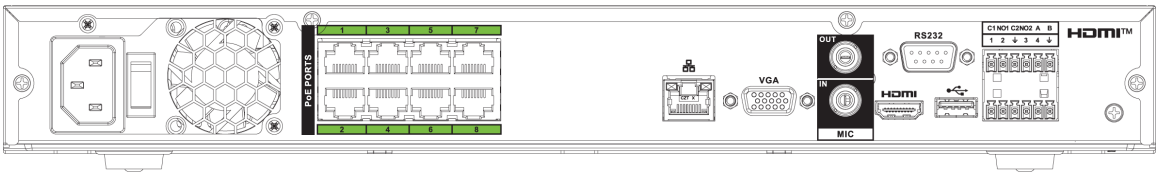
The NVR52-XI series rear panel is shown as below.

Figure 2-55 Rear panel



The NVR52-8P-XI series rear panel is shown as below.

Figure 2-56 Rear panel



The NVR52-16P-XI series rear panel is shown as below.

Figure 2-57 Rear panel

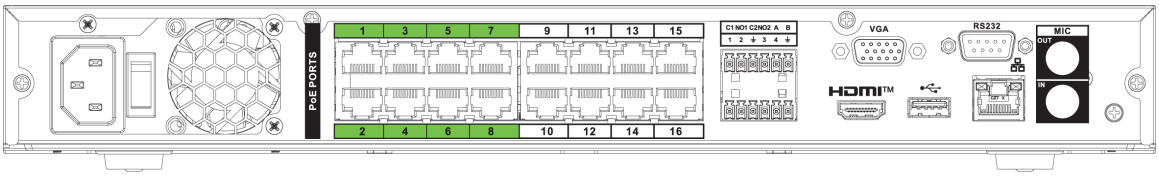


Table 2-21 Ports

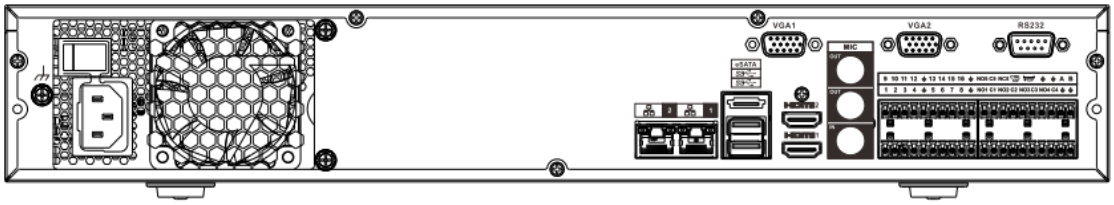
Icon	Port Name	Function
	Network port	10/100/1000 Mbps self-adaptive Ethernet port. Connect to the network cable.
HDMI	High Definition Media Page	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
SS	USB port	Connect to mouse, USB storage device, USB burner and more.

Icon	Port Name	Function
RS-232	RS-232 debug COM	It is for general COM debug to configure IP address or transfer transparent COM data.
VGA	VGA video output port	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video.
MIC IN	Audio input port	Bidirectional talk input port. It is to receive the analog audio signal output from the devices such as microphone, pickup.
MIC OUT	Audio output port	Audio output port. It is to output the analog audio signal to the devices such as the sound box. ● Bidirectional talk output. ● Audio output on 1-window video monitor. ● Audio output on 1-window video playback.
1–8	Alarm input port 1–8	● There are two groups. The first group is from port 1 to port 4; the second group is from port 5 to port 8. They are to receive the signal from the external alarm source. There are two types; NO (normal open)/NC (normal close). ● When your alarm input device is using external power, please make sure the device and the NVR have the same ground.
⏚	GND	Alarm input ground port.
NO1–NO3	Alarm output port 1–3	● 3 groups of alarm output ports. (Group 1: port NO1–C1; Group 2: port NO2–C2; Group 3: port NO3–C3). Output alarm signal to the alarm device. Please make sure there is power to the external alarm device. ● NO: Normal open alarm output port. ● C: Alarm output public end.
C1–C3		
A	RS-485 communication port	RS485_A port. It is the cable A. You can connect to the control devices such as speed dome PTZ.
B		RS485_B. It is the cable B. You can connect to the control devices such as speed dome PTZ.
DC 12V	Power input port	Input 12 VDC/4 A.
Power Switch	—	Power on/off button.
PoE PORTS	—	Built-in Switch. Support PoE or ePoE function. ● For ePoE series product, port 1 to port 8 are the ePoE ports. ePoE port supports 300 meters@100 Mbps, 800 meters@10 Mbps. Port 9 to port 16 are general PoE ports. ● The 8 PoE series product supports total 130 W. ● The 16 PoE series product supports total 130 W.

2.2.6 NVR54-4KS2/NVR58-4KS2/NVR54-16P-4KS2/ NVR58-16P-4KS2/NVR54-24P-4KS2/NVR58-16P-4KS2E

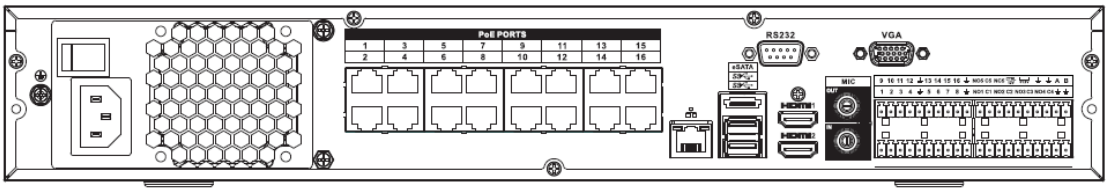
The NVR54-4KS2/NVR58-4KS2 series rear panel is shown as below.

Figure 2-58 Rear panel



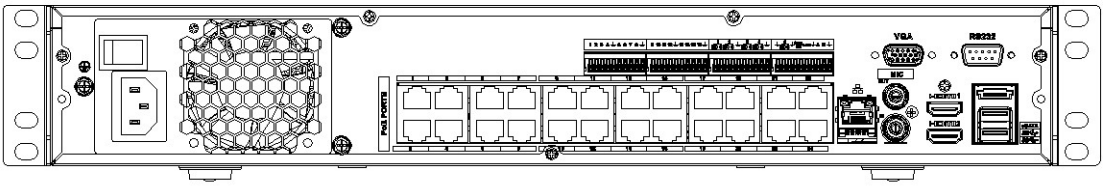
The NVR54-16P-4KS2/NVR58-16P-4KS2 series rear panel is shown as below.

Figure 2-59 Rear panel



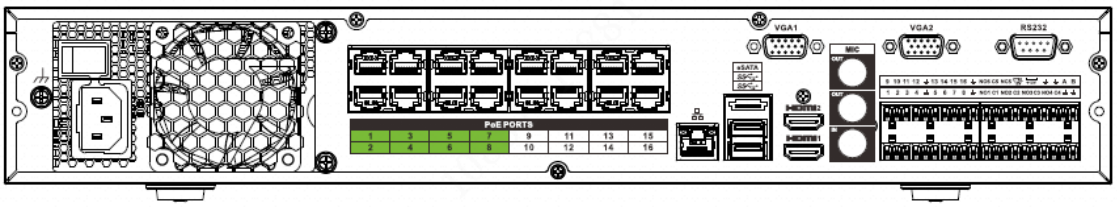
The NVR54-24P-4KS2 series rear panel is shown as below.

Figure 2-60 Rear panel



The NVR54-16P-4KS2E series rear panel is shown as below.

Figure 2-61 Rear panel



The NVR58-16P-4KS2E series rear panel is shown as below.

Figure 2-62 Rear panel

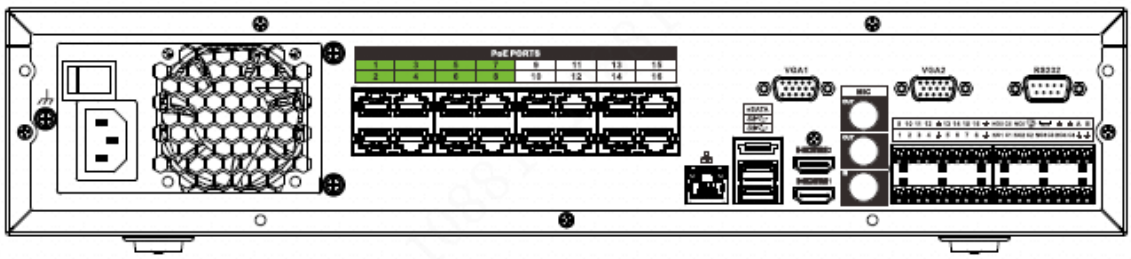
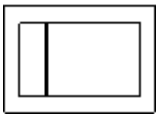
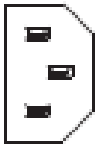
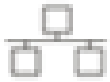


Table 2-22 Rear panel description

Name		Function
	Power switch	Power on-off button.
	Power input port	Input 100–240 VAC.
	Network port	10/100/1000 Mbps self-adaptive Ethernet port. Connect to the network cable.
eSATA	eSATA port	External SATA port. It can connect to the device of the SATA port. Please jump the HDD when there is peripheral connected HDD.
	USB port	USB port. Connect to mouse, USB storage device, USB burner and more.
HDMI	High Definition Media Page	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4b.
MIC IN	Audio input port	Bidirectional talk input port. It is to receive the analog audio signal output from the devices such as microphone, pickup.
MIC OUT	Audio output port	Audio output port. It is to output the analog audio signal to the devices such as the sound box. ● Bidirectional talk output. ● Audio output on 1-window video monitor. ● Audio output on 1-window video playback.

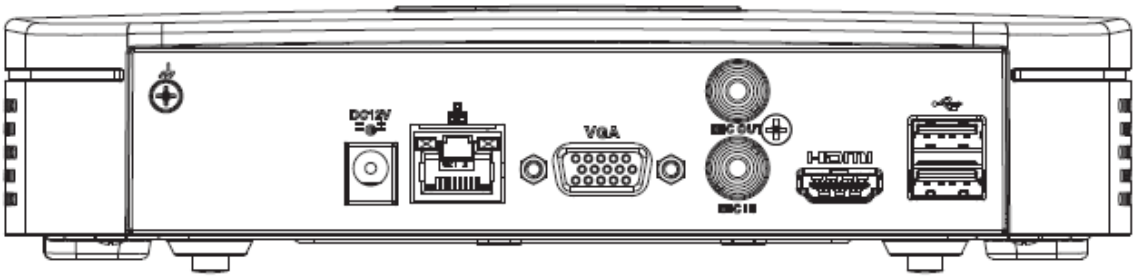
Name		Function
1–16	Alarm input port 1–16	• There are four groups. The first group is from port 1 to port 4, the second group is from port 5 to port 8, the third group is from 9 to 12, and the fourth group is from 13 to 16. They are to receive the signal from the external alarm source. There are two types; NO (normal open)/NC (normal close). • When your alarm input device is using external power, please make sure the device and the NVR have the same ground.
⏚	Ground	Alarm input ground end.
NO1–NO5 C1–C5 NC5	Alarm output port 1–5	• 5 groups of alarm output ports. (Group 1: port NO1–C1, Group 2: port NO2–C2, Group 3: port NO3–C3, Group 4: port NO4–C4, Group 5: port NO5, C5, NC5). Output alarm signal to the alarm device. Please make sure there is power to the external alarm device. • NO: Normal open alarm output port. • C: Alarm output public end. • NC: Normal close alarm output port.
A	RS-485 communication port	RS485_A port. It is the cable A. You can connect to the control devices such as speed dome PTZ.
B		RS485_B. It is the cable B. You can connect to the control devices such as speed dome PTZ.
CTRL (CTRL 12 V)	—	Controller 12 V power output. It is to control the on-off alarm relay output. It can be used to control the device alarm output. At the same time, it can also be used as the power input source of some devices such as the alarm detector.
P (+12 V)	—	+12 V power output port. It can provide the power to some peripheral devices such as the camera or the alarm device. Please note the supplying power shall be below 1 A.
RS-232	RS-232 debug COM	It is for general COM debug to configure IP address or transfer transparent COM data.
VGA	VGA video output port	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video.
PoE PORTS	—	Built-in Switch. Support PoE or ePoE function. For ePoE series product, port 1 to port 8 are the ePoE ports. ePoE port supports 300 meters@100 Mbps, 800 meters@10 Mbps. Port 9 to port 16 are general PoE ports. The 16 PoE series supports total 150 W.

The two ports serve as another group of alarm output ports.

2.2.7 NVR41-4KS2/NVR41-P-4KS2/NVR41-8P-4KS2/ NVR41-4KS2/L/NVR41-P-4KS2/L/NVR41-8P-4KS2/L/NVR21-S3/NVR21-P-S3/NVR21-8P-S3

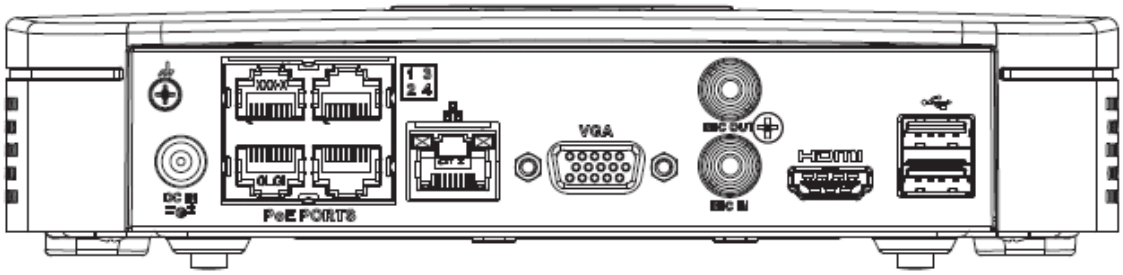
The NVR41-4KS2/NVR41-4KS2/L/NVR21-S3 series rear panel is shown as below.

Figure 2-63 Rear panel



The NVR41-P-4KS2/NVR41-P-4KS2/L series rear panel is shown as below.

Figure 2-64 Rear panel



The NVR41-8P-4KS2/NVR41-8P-4KS2/L series rear panel is shown as below.

Figure 2-65

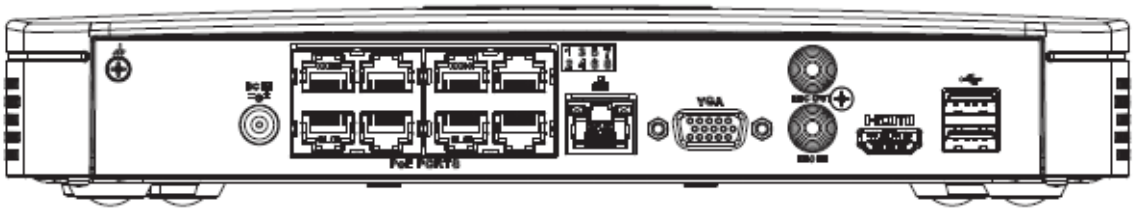


Table 2-23 Ports

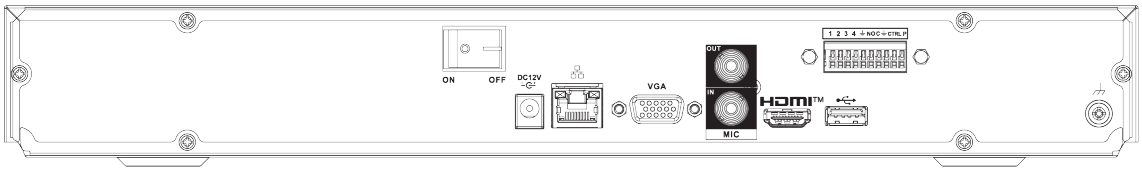
Port Name	Connection	Function
	USB port	USB port. Connect to mouse, USB storage device, USB burner and more.
	Network port	10/100 Mbps self-adaptive Ethernet port. Connect to the network cable.

Port Name	Connection	Function
HDMI	High Definition Media Page	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
VGA	VGA video output port	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video.
⏚	GND	Ground end.
DC 12V / DC IN	Power input port	Power socket. ● For NVR41-4KS2: 12 VDC/2 A power. ● For NVR41-P-4KS2: 48 VDC/72 W power. ● For NVR41-8P-4KS2: 48 VDC/96 W power.
MIC IN	Audio input port	Bidirectional talk input port. It is to receive the analog audio signal output from the devices such as microphone, pickup.
MIC OUT	Audio output port	Audio output port. It is to output the analog audio signal to the devices such as the sound box. ● Bidirectional talk output. ● Audio output on 1-window video monitor. ● Audio output on 1-window video playback.
PoE PORTS	PoE port	Built-in switch. Support PoE function. For PoE series product, you can use this port to provide power to the network camera.

2.2.8 NVR42-4KS2/NVR42-P-4KS2/NVR42-8P-4KS2/ NVR42-16P-4KS2/NVR42-4KS2/L/NVR42-P-4KS2/L/ NVR42-8P-4KS2/L/NVR42-16P-4KS2/L/NVR42-EI/NVR42-P-EI/NVR42-8P-EI/NVR42-4KS3/NVR42-P-4KS3/ NVR42-8P-4KS3/NVR42-16P-4KS3 Series

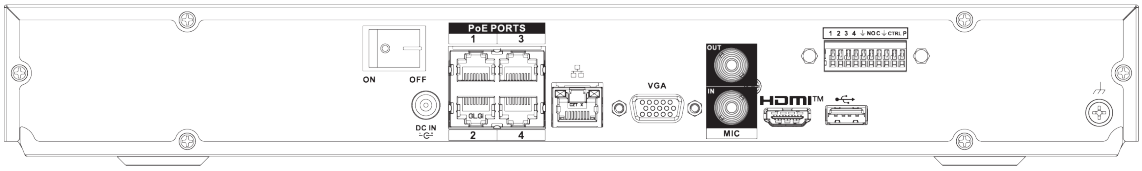
The NVR42-4KS2/NVR42-4KS2/L/NVR42-EI/NVR42-4KS3 series rear panel is shown as below.

Figure 2-66 Rear panel



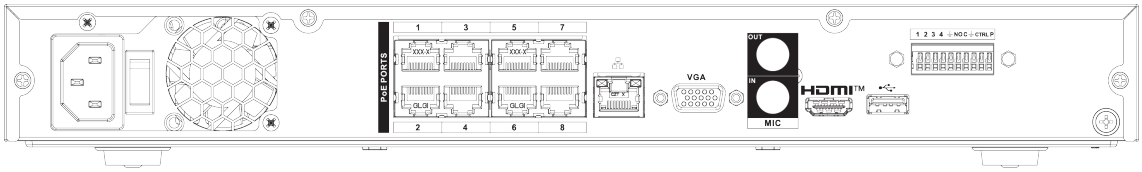
The NVR42-P-4KS2/NVR42-P-4KS2/L/NVR42-P-EI/NVR42-P-4KS3 series rear panel is shown as below.

Figure 2-67 Rear panel



The NVR42-8P-4KS2/NVR42-8P-4KS2/L/NVR42-8P-EI/NVR42-8P-4KS3 series rear panel is shown as below.

Figure 2-68 Rear panel



The NVR42-16P-4KS2/NVR42-16P-4KS2/L/NVR42-16P-4KS3 series rear panel is shown as below.

Figure 2-69 Rear panel

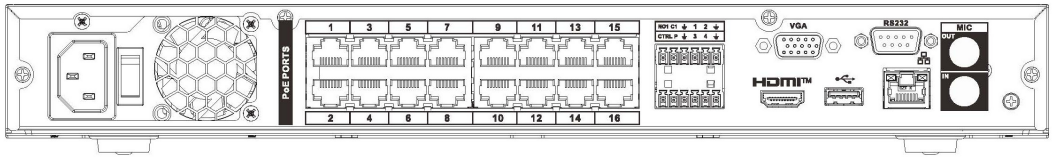


Table 2-24 Rear panel description

Name		Function
	Power switch	Power on/off button.
DC 12V / DC IN	Power input port	Power socket. ● For NVR42-4KS2/NVR42-EI/NVR42-4KS3 series, input 12 VDC/4 A. ● For NVR42-P-4KS2 series, input 48 VDC/96 W. ● For NVR42-P-EI/NVR42-P-4KS3 series, input 53 VDC/1.81 A.
		Input 90~264-12 VAC 5 A/52 V 2.5 A-190 W. For NVR42-8P-4KS2/NVR42-16P-4KS2/NVR42-8P-EI/ NVR42-8P-4KS3/NVR42-16P-4KS3 series product only.
MIC IN	Audio input port	Bidirectional talk input port. It is to receive the analog audio signal output from the devices such as microphone, pickup.

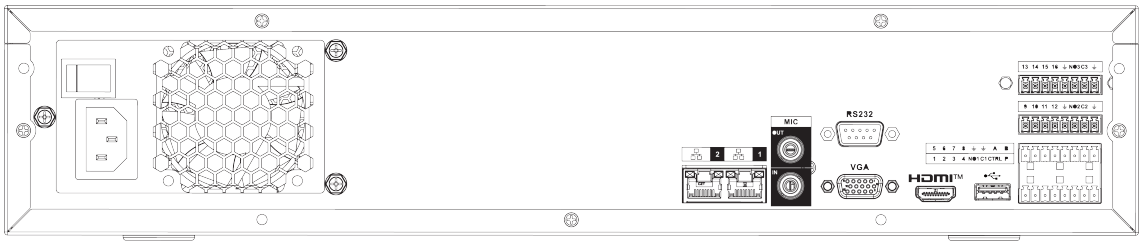
Name		Function
MIC OUT	Audio output port	Audio output port. It is to output the analog audio signal to the devices such as the sound box. ● Bidirectional talk output. ● Audio output on 1-window video monitor. ● Audio output on 1-window video playback.
1–4	Alarm input port 1–4	● There are two types; NO (normal open)/NC (normal close). ● When your alarm input device is using external power, please make sure the device and the NVR have the same ground.
⏚	GND	Alarm input ground port.
N1, N2	Alarm output port 1–2	● 2 groups of alarm output ports. (Group 1: port NO1–C1, Group 2: port NO2–C2). Output alarm signal to the alarm device. Please make sure there is power to the external alarm device. ● NO: Normal open alarm output port. ● C:Alarm output public end.
C1, C2		
A	RS-485 communication port	RS485_A port. It is the cable A. You can connect to the control devices such as speed dome PTZ.
B		RS485_B. It is the cable B. You can connect to the control devices such as speed dome PTZ.
🖧	Network port	10/100/1000 Mbps self-adaptive Ethernet port. Connect to the network cable.
⇆	USB port	USB port. Connect to mouse, USB storage device, USB burner and more.
RS-232	RS-232 debug COM	It is for general COM debug to configure IP address or transfer transparent COM data.
HDMI	High Definition Media Page	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.4.
VGA	VGA video output port	VGA video output port. Output analog video signal. It can connect to the monitor to view analog video.
PoE PORTS	/	Built-in Switch. Support PoE. For PoE series product, you can use this port to provide power to the network camera.

2.2.9 NVR44-4KS2/NVR44-16P-4KS2/NVR44-4KS2/L/ NVR44-16P-4KS2/L/NVR44-4KS2/I/NVR44-16P-4KS2/I/

NVR48-EI/NVR44-EI/NVR48-16P-EI/NVR44-16P-EI/ NVR44-4KS3/NVR48-4KS3 Series

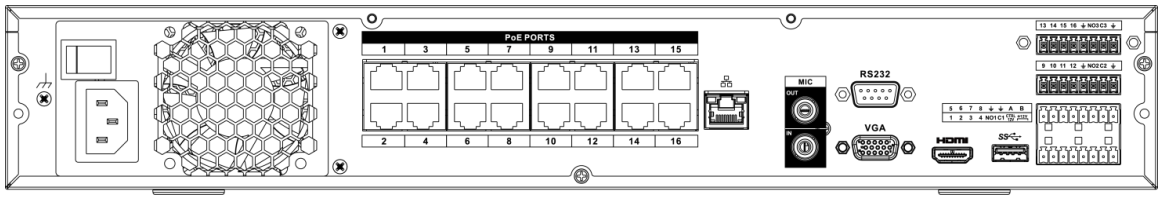
The NVR44-4KS2/NVR44-4KS2/L/NVR44-4KS2/I/NVR48-EI/NVR44-EI/NVR44-4KS3/NVR48-4KS3 series rear panel is shown as below.

Figure 2-70 Rear panel



The NVR44-16P-4KS2/NVR44-16P-4KS2/L/NVR44-16P-4KS2/I series rear panel is shown as below.

Figure 2-71 Rear panel



The NVR48-16P-EI/NVR44-16P-EI series rear panel is shown as below.

Figure 2-72 Rear panel

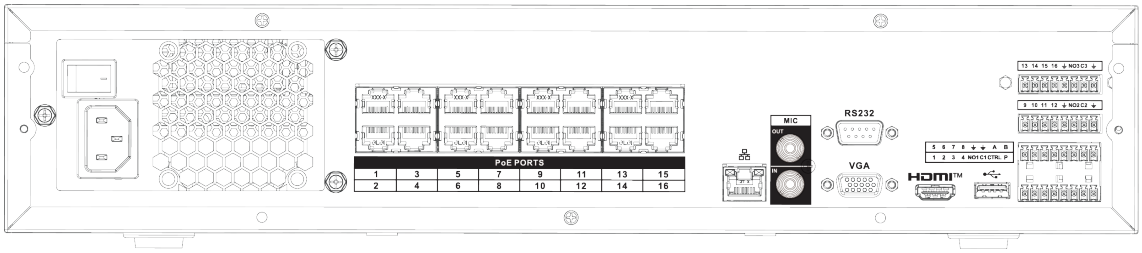


Table 2-25 Ports

Name		Function
Power switch	—	Power on-off button.
Power input port	—	90~264-12 VAC 12.5 A/-53 V 2.83 A.
MIC IN	Audio input port	Bidirectional talk input port. It is to receive the analog audio signal output from the devices such as microphone, pickup.
MIC OUT	Audio output port	Audio output port. It is to output the analog audio signal to the devices such as the sound box. ● Bidirectional talk output. ● Audio output on 1-window video monitor. ● Audio output on 1-window video playback.

Name		Function	
VIDEO OUT	Video output port	CVBS output.	
1–16	Alarm input port 1–16	• There are four groups. The first group is from port 1 to port 4, the second group is from port 5 to port 8, the third group is from 9 to 12, and the fourth group is from 13 to 16. They are to receive the signal from the external alarm source. There are two types; NO (normal open)/NC (normal close). • When your alarm input device is using external power, please make sure the device and the NVR have the same ground.	
⏚	Video output port	CVBS output.	
NO1–NO3	Alarm output port 1–3	• 3 groups of alarm output ports. (Group 1: port NO1–C1; Group 2: port NO2–C2; Group 3: port NO3–C3). Output alarm signal to the alarm device. Please make sure there is power to the external alarm device. • NO: Normal open alarm output port. • C: Alarm output public end.	
C1–C3			
A	RS-485 communication port	RS485_A port. It is the cable A. You can connect to the control devices such as speed dome PTZ.	
B		RS485_B. It is the cable B. You can connect to the control devices such as speed dome PTZ.	
CTRL (CTRL 12 V)	—	Controller 12 V power output. It is to control the on-off alarm relay output. It can be used to control the device alarm output. At the same time, it can also be used as the power input source of some devices such as the alarm detector.	📖 The two ports serve as another group of alarm output ports.
P (+12 V)	—	+12 V power output port. It can provide the power to some peripheral devices such as the camera or the alarm device. Please note the supplying power shall be below 1 A.	
🖧	Network port	10/100/1000 Mbps self-adaptive Ethernet port. Connect to the network cable.	
eSATA	eSATA port	External SATA port. It can connect to the device of the SATA port. Please jump the HDD when there is peripheral connected HDD.	
⇆	USB 2.0 port	USB 2.0 port. Connect to mouse, USB storage device, USB burner and more.	
RS-232	RS-232 debug COM	It is for general COM debug to configure IP address or transfer transparent COM data.	
HDMI	High Definition Media Page	High definition audio and video signal output port. It transmits uncompressed high definition video and multiple-channel data to the HDMI port of the display device. HDMI version is 1.3.	

Figure 5-129 Search by attributes

Step 2 Select the channel and set the parameters including start time, end time, gender, age, glasses, beard, mask, name and similarity.

Step 3 Click **Search**.

The faces in the image are intentionally blurred for privacy protection. The actual images are clear.

Figure 5-130 Search results

Related Operations

- Play back video.

  Click an image, and then click to play back the related video.

During playback, you can:

- ◇ Click to pause.
- ◇ Click to stop.
- ◇ Click to display AI rule. The icon changes to .

- Add tags.

  Select one or more images, and then click **Add Tag**.
- Lock.

  Select one or more images, and then click **Lock**. The locked files will not be overwritten.
- Export.

  Select one or more images, and then click **Export** to export selected search results in excel.
- Back up.

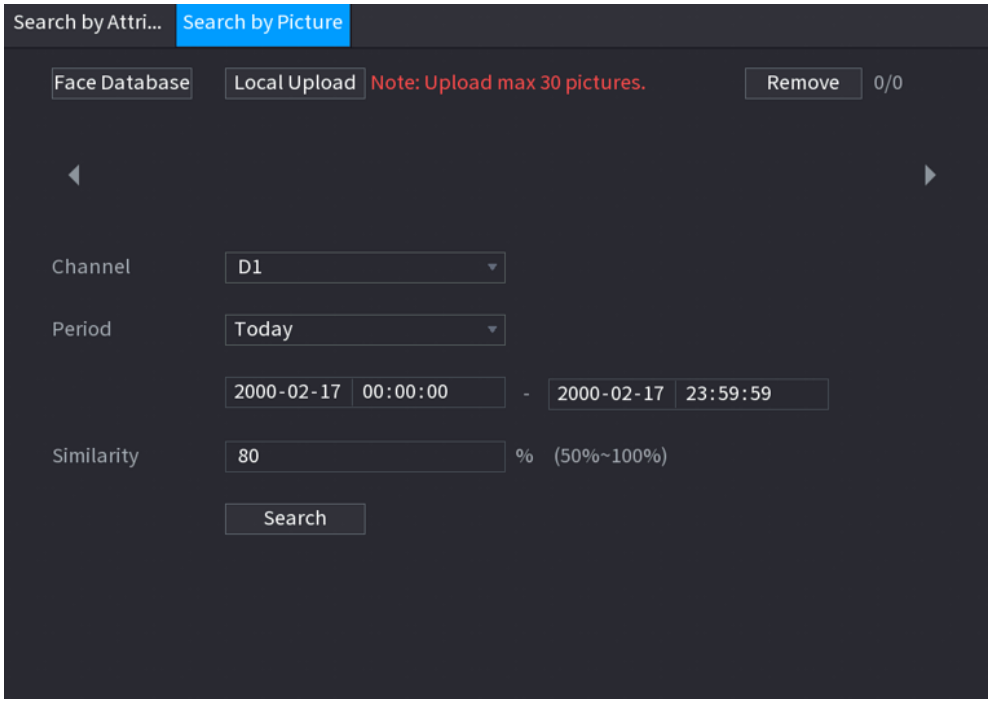
  Select one or more images, click **Backup** , select the storage path and file type, and then click **Start** to export files to external storage device.

5.9.6.5.2 Search by Image

Procedure

Step 1 Select **Main Menu** > **AI** > **AI Search** > **Face Recognition** > **Search by Picture**.

Figure 5-131 Search by image



Step 2 Upload face images.

- **Face Database** : Upload face images from database.
- **Local Upload** : Upload face images from external storage device.

Step 3 Select the image used to search and then set the parameters including channel, start time, end time, gender, age, glasses, beard, mask, and similarity.

Step 4 Click **Search**.

The search results are displayed.

Related Operations

- Play back video.

  Click an image, and then click to play back the related video.

  During playback, you can:

  - Click to pause.
  - Click to stop.
  - Click to display AI rule. The icon changes to .
- Add tags.

  Select one or more images, and then click **Add Tag**.
- Lock.

  Select one or more images, and then click **Lock**. The locked files will not be overwritten.
- Export.

  Select one or more images, and then click **Export** to export selected search results in excel.
- Back up.

  Select one or more images, click **Backup** , select the storage path and file type, and then click **Start** to export files to external storage device.

5.9.6.5.3 Report Query

Background Information

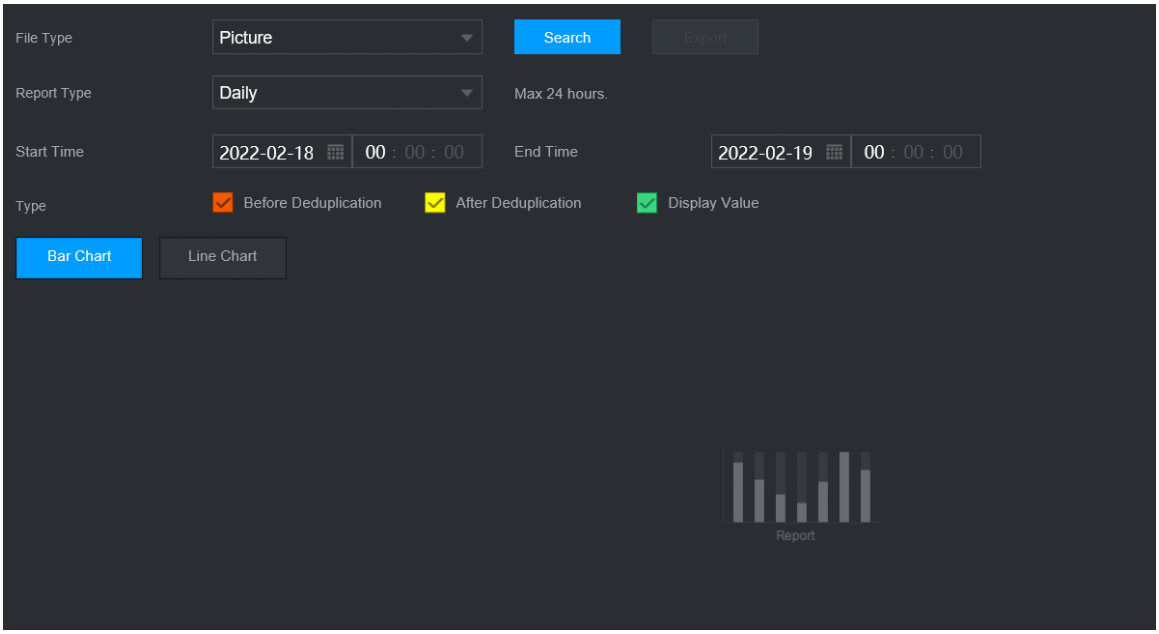
You can search for and export face statistics.

- The statistics might be overwritten when the storage space runs out. Back up in time.
- When you restore the Device to factory settings, all the data except data in the external storage device will be cleared. You can clear the data in the external storage device through formatting or other methods.

Procedure

Step 1 Select **Main Menu** > **AI** > **Report Query** > **Face Statistics**.

Figure 5-132 Face statistics



Step 2 Select the report type, start time and end time, and then click **Search**.

Related Operations

- Switch chart type.

  Click **Bart Chart** or **Line Chart** to switch the chart type.
- Export.

  Select file type, and then click **Export** to export the report in picture or csv format.

5.9.7 IVS

The IVS function processes and analyzes the images to extract the key information to match the specified rules. When the detected behaviors match the rules, the system activates alarms.

- This function is available on select models.
- IVS and face detection cannot be enabled at the same time.

5.9.7.1 Enabling Smart Plan

To use AI by camera, you need to enable the smart plan first. For details, see "5.9.3 Smart Plan".

5.9.7.2 Configuring IVS

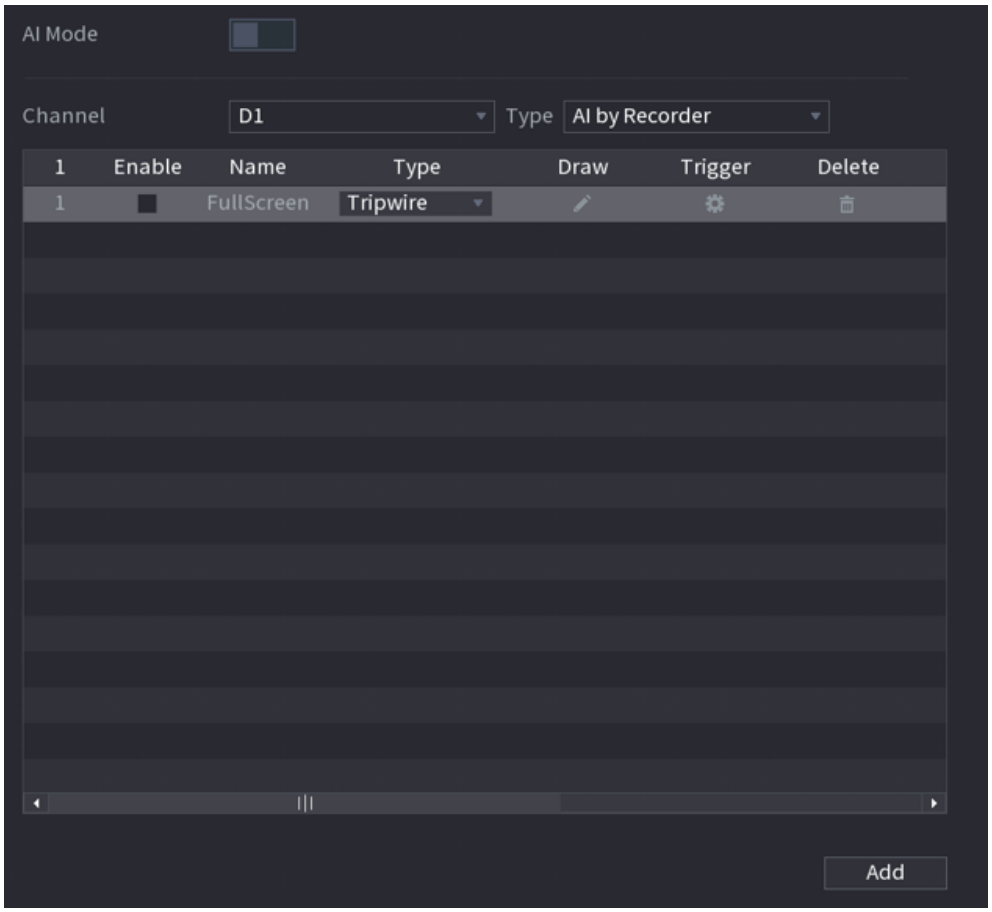
5.9.7.2.1 Tripwire

When the detection target crosses the warning line along the set direction, the system performs an alarm linkage action.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameters** > **IVS**.

Figure 5-133 IVS



Step 2 Select the channel and AI type.

Step 3 Click **Add** to add a rule.

Step 4 On the **Type** list, select **Tripwire**.

Step 5 Draw the detection rule.

1. Click to draw a straight line or a curve on the surveillance video image. Right-click the image to stop drawing.

Figure 5-134 Tripwire (AI by camera)

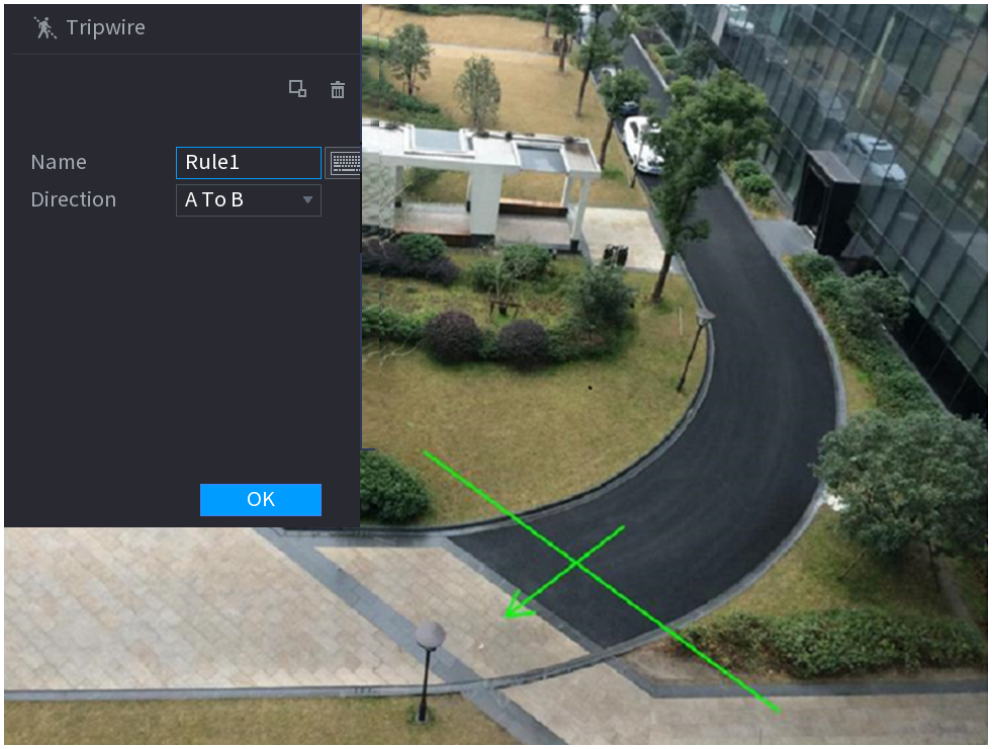
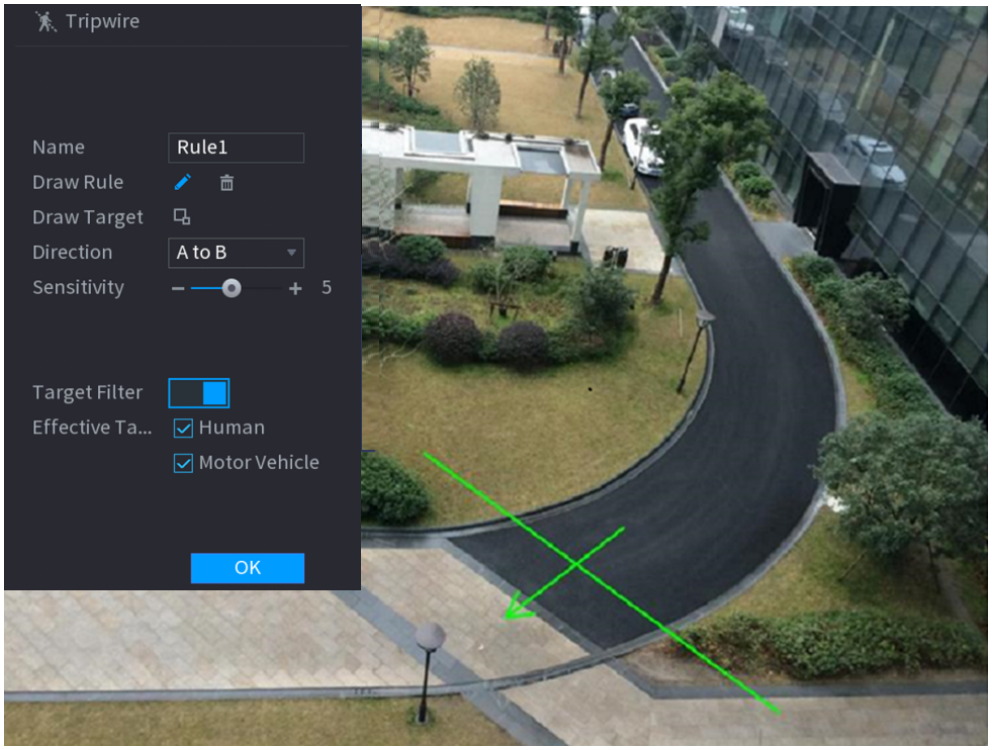


Figure 5-135 Tripwire (AI by recorder)



2. Click to draw the minimum size or maximum size to filter the target.

   The system triggers an alarm only when the size of detected target is between the maximum size and the minimum size.
3. Configure the parameters.

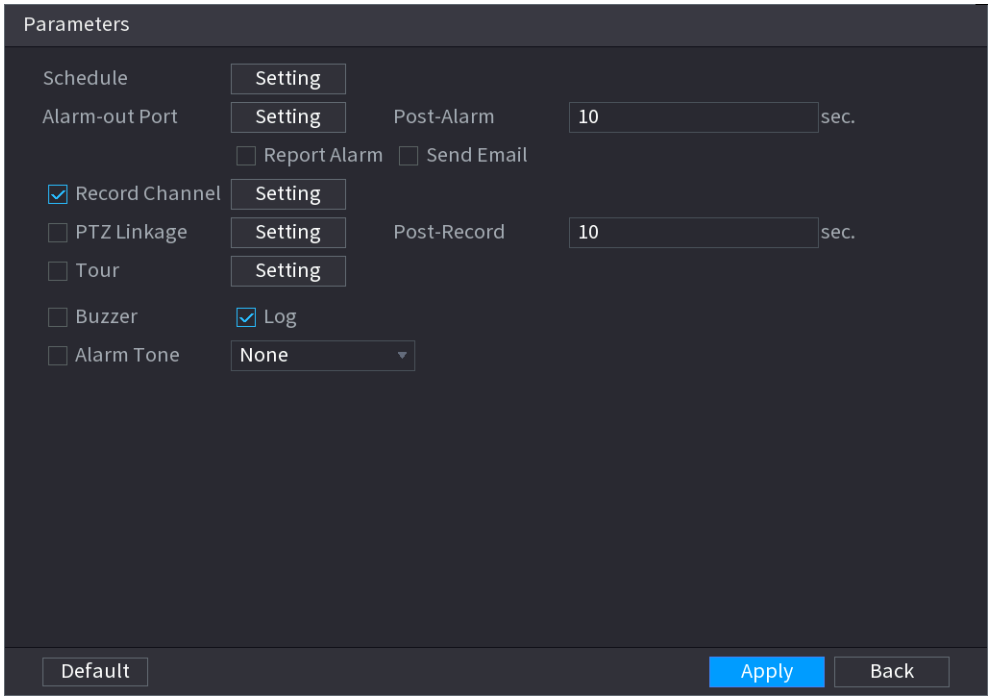
Table 5-33 Tripwire parameters

Parameter	Description
Name	Customize the rule name.
Direction	Set the tripwire direction, including A→B, B→A and A↔B.
Target Filter	Click and then select effective target. With **Human** and **Motor Vehicle** selected by default, the system automatically identifies the person and motor vehicle appeared within the monitoring range.

4. Click **OK**.

Step 6 Configure alarm schedule and linkage.

Figure 5-136 Schedule and alarm linkage



1. Click .
2. Click **Setting** next to **Schedule** to configure the alarm period.

   The system performs linkage actions only for alarms during the arming period.

   - On the time line, drag to set the period.
   - You can also click to set the period.
3. Configure alarm linkage. For details, see Table 5-50 .
4. Click **Apply**.

Step 7 Select the **Enable** checkbox and then click **Apply**.

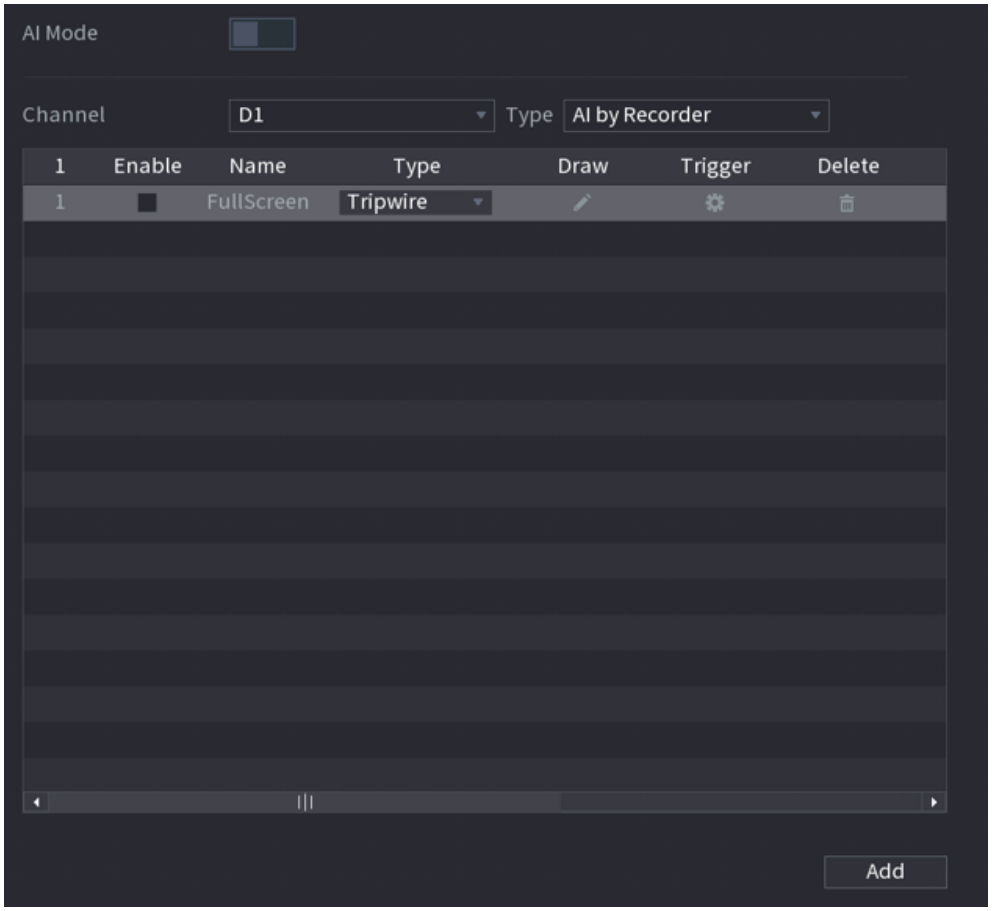
5.9.7.2.2 Intrusion

When the detection target passes the edge of the monitoring area, and enters, leaves or traverses the monitoring area, the system performs an alarm linkage action.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameters** > **IVS**.

Figure 5-137 IVS



Step 2 Select the channel and AI type.

Step 3 Click **Add** to add a rule.

Step 4 On the **Type** list, select **Intrusion**.

Step 5 Draw the detection rule.

1. Click to draw the rule on the surveillance video image. Right-click the image to stop drawing.

Figure 5-138 Intrusion (AI by camera)

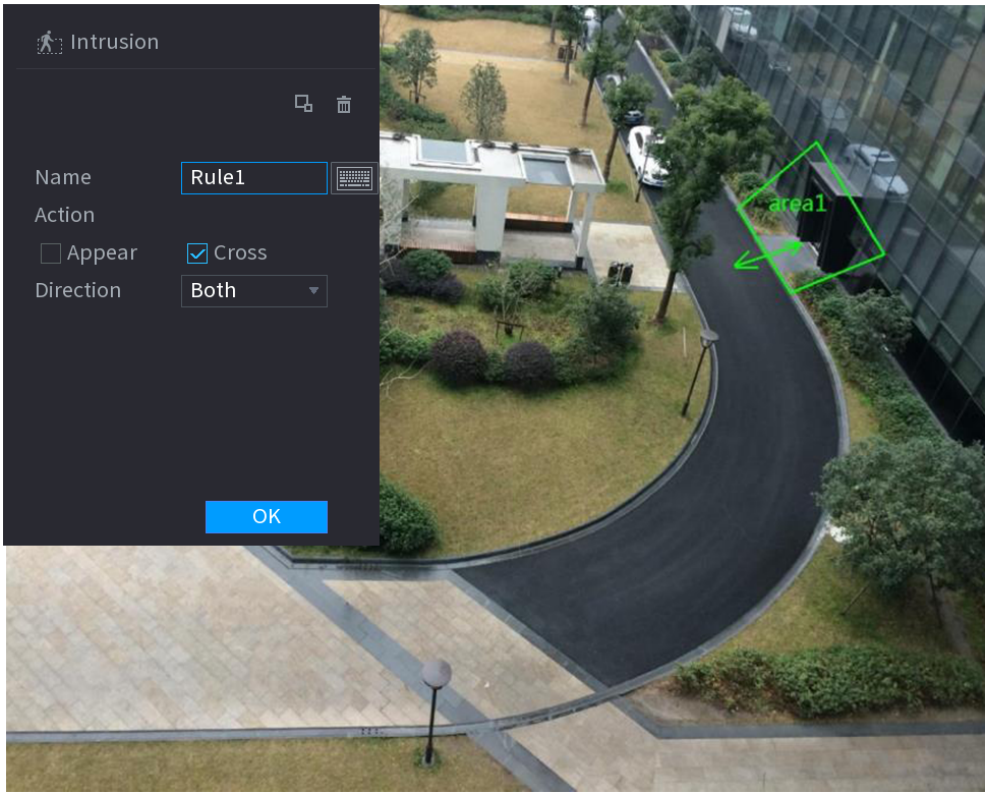
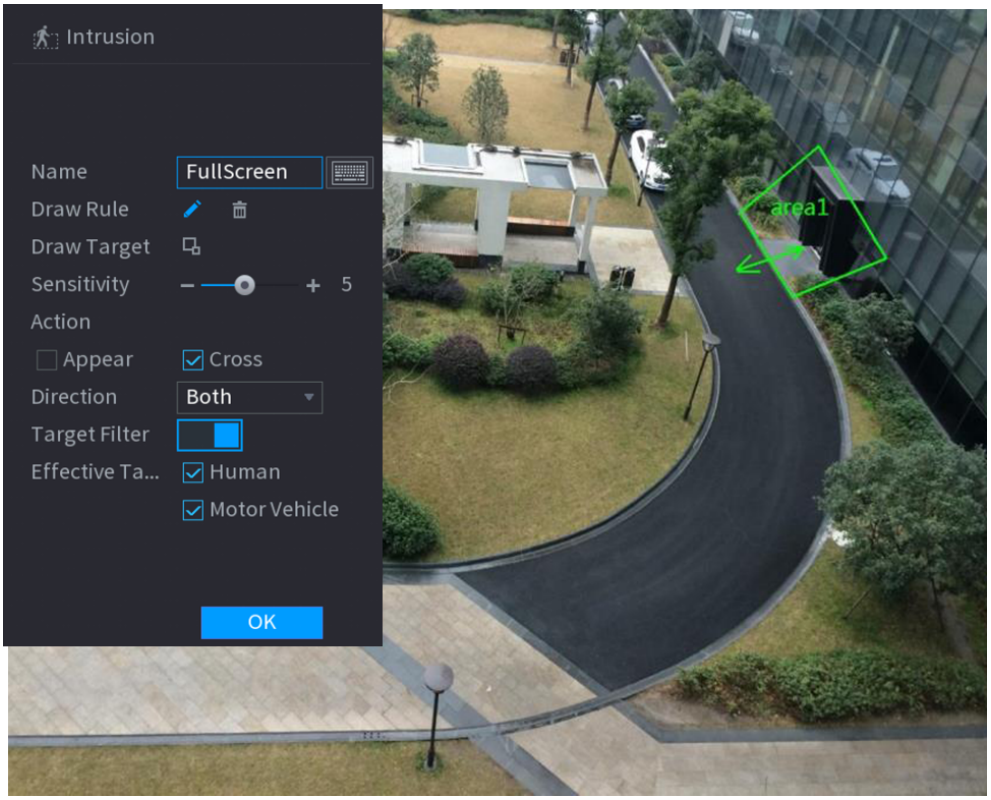


Figure 5-139 Intrusion (AI by recorder)



2. Click to draw the minimum size or maximum size to filter the target.

The system triggers an alarm only when the size of detected target is between the maximum size and the minimum size.

3. Configure the parameters.

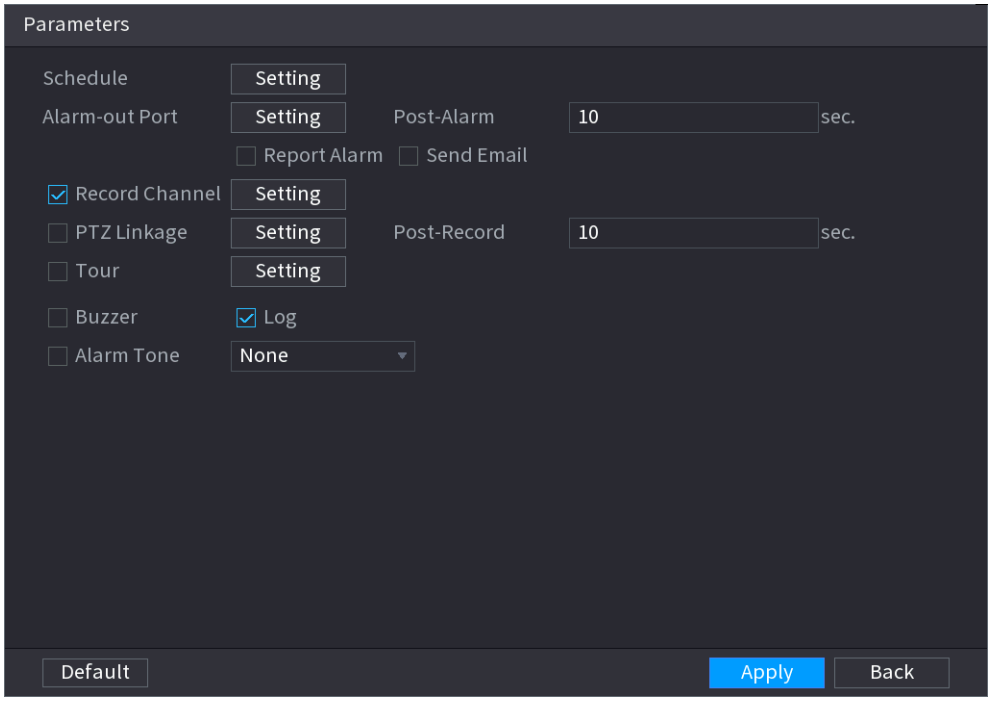
Table 5-34 Intrusion parameters

Parameter	Description
Name	Customize the rule name.
Action	Set the intrusion action, including appear and crossing area.
Direction	Set the direction to cross the area, including enter, exit and both.
Target Filter	Click and then select effective target. With **Human** and **Motor Vehicle** selected by default, the system automatically identifies the person and motor vehicle appeared within the monitoring range.

4. Click **OK**.

Step 6 Configure alarm schedule and linkage.

Figure 5-140 Schedule and alarm linkage



1. Click .
2. Click **Setting** next to **Schedule** to configure the alarm period.

   The system performs linkage actions only for alarms during the arming period.

   - On the time line, drag to set the period.
   - You can also click to set the period.
3. Configure alarm linkage. For details, see Table 5-50 .
4. Click **Apply**.

Step 7 Select **Enable** checkbox and then click **Apply**.

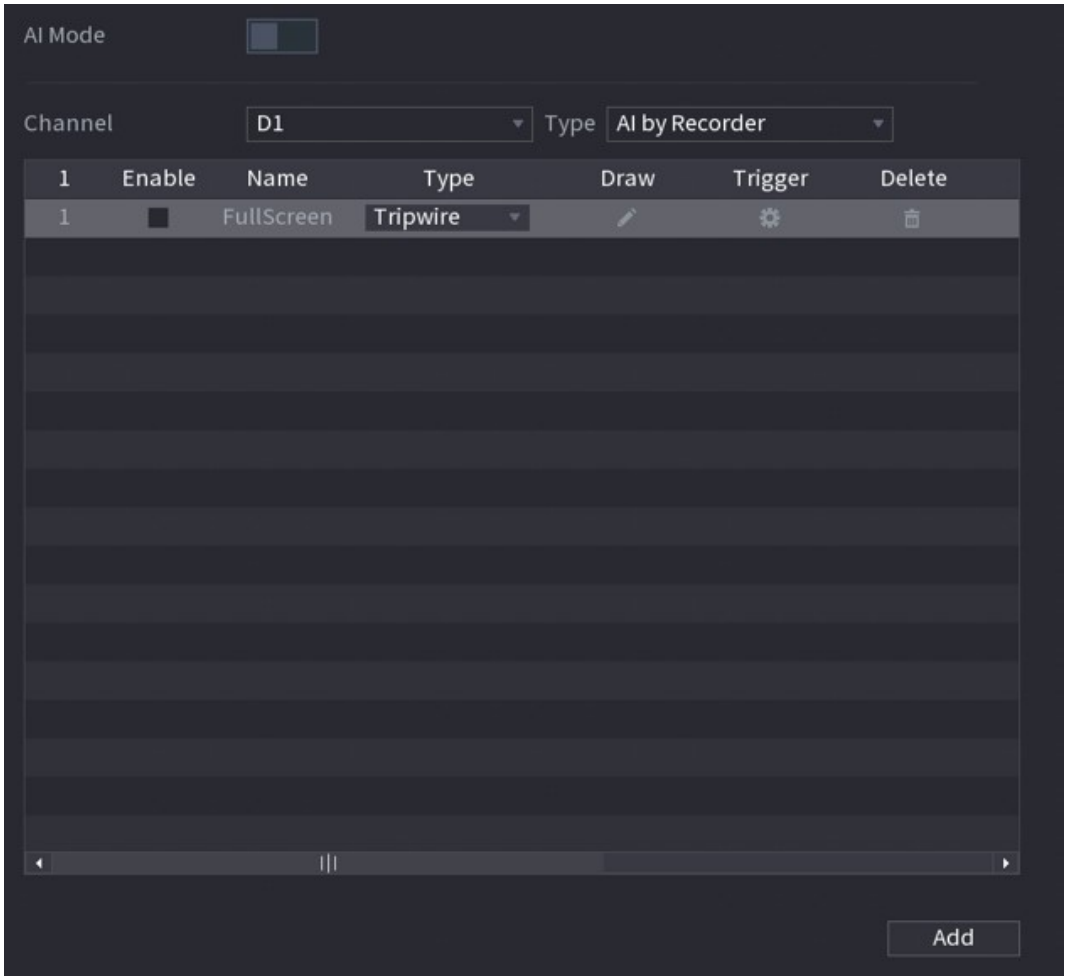
5.9.7.2.3 Abandoned Object Detection

The system generates an alarm when there is an abandoned object in the specified zone.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameters** > **IVS**.

Figure 5-141 IVS



Step 2 Select channel and AI type.

Step 3 Click **Add** to add a rule.

Step 4 On the **Type** list, select **Abandoned Object**.

Step 5 Draw the detection rule.

1. Click to draw a rectangle on the surveillance video image. Right-click the image to stop drawing.

Figure 5-154 Missing object

2. Click to draw the minimum size or maximum size to filter the target.

   The system triggers an alarm only when the size of detected target is between the maximum size and the minimum size.
3. Configure parameters.

Table 5-39 Parameters of missing object detection

Parameter	Description
Preset	Set the preset point for IVS detection according to the actual needs.
Name	Customize the rule name.
Duration	Set how long the object stays until the alarm is triggered.

4. Click **OK**.

Step 6 Configure alarm schedule and linkage.

Figure 5-155 Schedule and alarm linkage

1. Click .
2. Click **Setting** next to **Schedule** to configure the alarm period.

   The system performs linkage actions only for alarms during the arming period.

   - On the time line, drag to set the period.
   - You can also click to set the period.
3. Configure alarm linkage. For details, see Table 5-50 .
4. Click **Apply**.

Step 7 Select **Enable** checkbox and then click **Apply**.

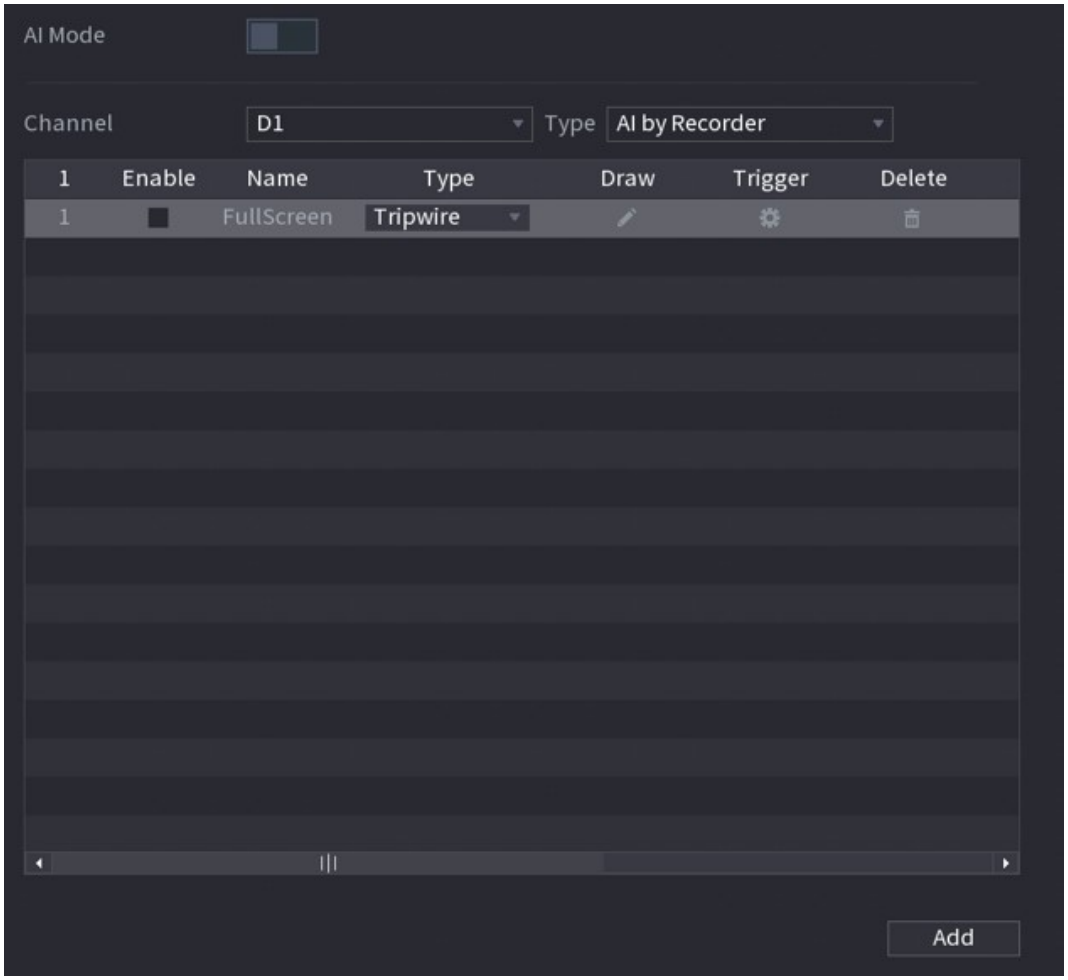
5.9.7.2.8 Loitering Detection

The system generates an alarm once the object is staying in the specified zone longer than the defined duration.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameters** > **IVS**.

Figure 5-156 IVS



Step 2 Select channel and AI type.

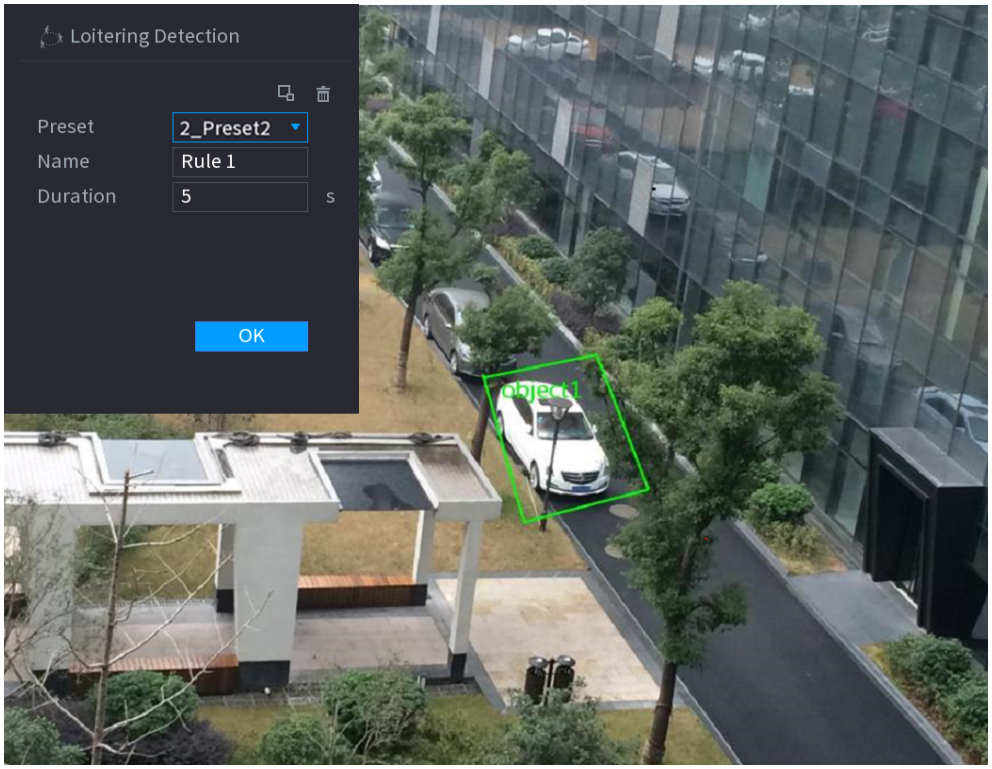
Step 3 Click **Add** to add a rule.

Step 4 On the **Type** list, select **Loitering Detection**.

Step 5 Draw the detection rule.

1. Click to draw a rectangle on the surveillance video image. Right-click the image to stop drawing.

Figure 5-157 Loitering detection



2. Click to draw the minimum size or maximum size to filter the target.

   The system triggers an alarm only when the size of detected target is between the maximum size and the minimum size.
3. Configure parameters.

Table 5-40 Loitering detection parameters

Parameter	Description
Preset	Set the preset point for IVS detection.
Name	Customize the rule name.
Duration	Set how long the object stays until the alarm is triggered.

4. Click **OK**.

Step 6 Configure alarm schedule and linkage.

Figure 5-158 Schedule and alarm linkage

1. Click .
2. Click **Setting** next to **Schedule** to configure the alarm period.

   The system performs linkage actions only for alarms during the arming period.

   - On the time line, drag to set the period.
   - You can also click to set the period.
3. Configure alarm linkage. For details, see Table 5-50 .
4. Click **Apply**.

Step 7 Select **Enable** checkbox and then click **Apply**.

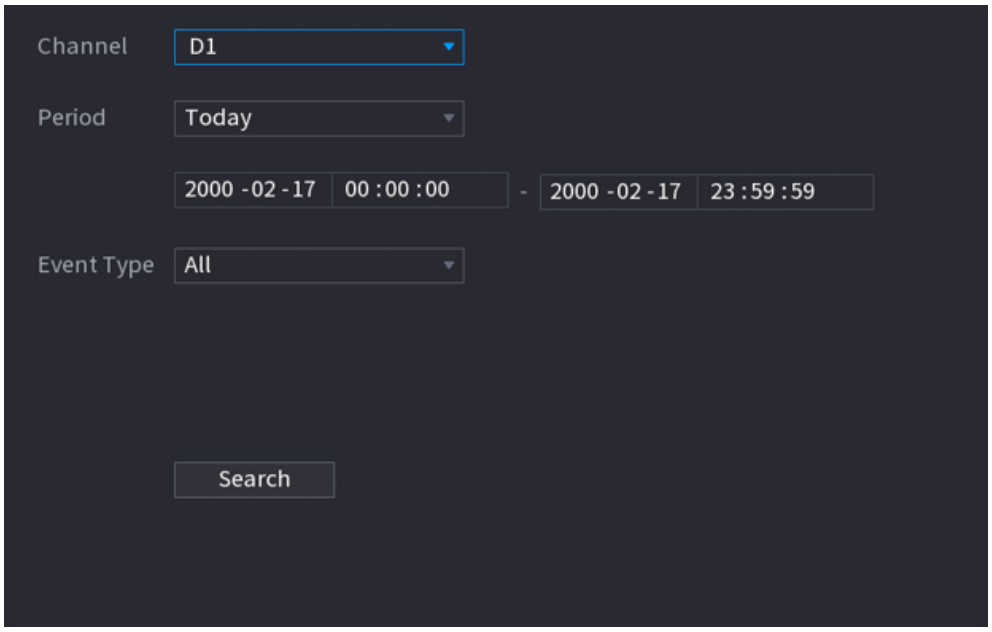
5.9.7.3 AI Search (IVS)

You can search for IVS detection results.

Procedure

Step 1 Select **Main Menu** > **AI** > **AI Search** > **IVS**.

Figure 5-159 IVS search



Step 2 Select a channel, start time, end time, event type, and then click **Search**.

The search results are displayed.

Related Operations

- Play back video.

  Click an image, and then click to play back the related video.

  During playback, you can:

  - Click to pause.
  - Click to stop.
  - Click to display AI rule. The icon changes to .
- Add tags.

  Select one or more images, and then click **Add Tag**.
- Lock.

  Select one or more images, and then click **Lock**. The locked files will not be overwritten.
- Export.

  Select one or more images, and then click **Export** to export selected search results in excel.
- Back up.

  Select one or more images, click **Backup** , select the storage path and file type, and then click **Start** to export files to external storage device.

5.9.8 Stereo Analysis

By drawing and setting the rules of stereo behavior analysis, the system will perform alarm linkage actions when the video matches the detection rule. Types of events include: people approach detection, fall detection, violence detection, people No. exception detection and people stay detection.

- This function requires access to a camera that supports stereo behavior analysis.
- Stereo analysis and IVS are mutually exclusive and cannot be enabled at the same time.

5.9.8.1 Enabling Smart Plan

To use AI by camera, you need to enable the smart plan first. For details, see "5.9.3 Smart Plan".

5.9.8.2 Configuring Stereo Analysis

5.9.8.2.1 People Approach Detection

When two people stay in the same detection area longer than the defined duration or when the distance between two people is larger or smaller than the defined threshold, an alarm will be triggered.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Stereo Analysis**.

Step 2 Select a channel and then click **Add**.

Step 3 Select **Enable** and then set **Type** to **People Approach Detection**.

Step 4 Draw detection rule.

1. Click , and then draw a detection area on the video image. Right-click the image to stop drawing.
2. Configure parameters.

Table 5-41 Parameters of people approach detection

Parameter	Description
Name	Customize the rule name.
Sensitivity	Set alarm sensitivity.
Duration	Set how long two people stay in the same detection area until an alarm is triggered.
Repeat Alarm Time	Set repeat alarm time. If the alarm-triggering event continues, an alarm will be triggered again when repeat alarm time passed.
Interval Threshold	When the distance between people in the area is greater than or less than the defined threshold, an alarm will be triggered.

3. Click **OK**.

Step 5 Configure alarm schedule and linkage.

Figure 5-160 Schedule and alarm linkage

1. Click .
2. Click **Setting** next to **Schedule** to configure the alarm period.

   The system performs linkage actions only for alarms during the arming period.

   - On the time line, drag to set the period.
   - You can also click to set the period.
3. Configure alarm linkage. For details, see Table 5-50 .
4. Click **Apply**.

Step 6 Click **Apply**.

5.9.8.2.2 Fall Detection

When someone falls from a height in the detection area and the duration of the action is greater than the defined threshold, an alarm will be triggered.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Stereo Analysis**.

Step 2 Select a channel and then click **Add**.

Step 3 Select **Enable** and then set **Type** to **Fall Detection**.

Step 4 Draw detection rule.

1. Click , and then draw a detection area on the video image. Right-click the image to stop drawing.
2. Configure parameters.

Table 5-42 Parameters of fall detection

Parameter	Description
Name	Customize the rule name.
Sensitivity	Set alarm sensitivity.
Duration	Set the minimum time of triggering an alarm when people fall.
Repeat Alarm Time	Set repeat alarm time. If the alarm-triggering event continues, an alarm will be triggered again when repeat alarm time passed.

3. Click **OK**.

Step 5 Configure alarm schedule and linkage.

Figure 5-161 Schedule and alarm linkage

1. Click .
2. Click **Setting** next to **Schedule** to configure the alarm period.

   The system performs linkage actions only for alarms during the arming period.

   - On the time line, drag to set the period.
   - You can also click to set the period.
3. Configure alarm linkage. For details, see Table 5-50 .
4. Click **Apply**.

Step 6 Click **Apply**.

5.9.8.2.3 Violence Detection

When the target in the detection region has large body movements such as smashing and fighting, an alarm will be triggered.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Stereo Analysis**.

Step 2 Select a channel and then click **Add**.

Step 3 Select **Enable** and then set **Type** to **Violence Detection**.

Step 4 Draw detection rule.

1. Click , and then draw a detection area on the video image. Right-click the image to stop drawing.
2. Configure parameters.

Table 5-43 Parameters of violence detection

Parameter	Description
Name	Customize the rule name.
Sensitivity	Set alarm sensitivity.

3. Click **OK**.

Step 5 Configure alarm schedule and linkage.

Figure 5-162 Schedule and alarm linkage

1. Click .
2. Click **Setting** next to **Schedule** to configure the alarm period.

   The system performs linkage actions only for alarms during the arming period.

   - On the time line, drag to set the period.
   - You can also click to set the period.
3. Configure alarm linkage. For details, see Table 5-50 .
4. Click **Apply**.

Step 6 Click **Apply**.

5.9.8.2.4 People No. Exception Detection

When the system detects an abnormal number of people in the same detection area, an alarm will be triggered.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Stereo Analysis**.

Step 2 Select a channel and then click **Add**.

Step 3 Select **Enable** and then set **Type** to **People No. Exception Detection**.

Step 4 Draw detection rule.

1. Click , and then draw a detection area on the video image. Right-click the image to stop drawing.
2. Configure parameters.

Table 5-44 Parameters of people No. exception detection

Parameter	Description
Name	Customize the rule name.
Sensitivity	Set alarm sensitivity.
Duration	Set the minimum time to trigger an alarm after the system detects an abnormal number of people.
Repeat Alarm Time	Set repeat alarm time. If the alarm-triggering event continues, an alarm will be triggered again when repeat alarm time passed.
Alarm People No.	When the number of people in the area is greater than, equal to, or less than the defined threshold, an alarm will be triggered.

3. Click **OK**.

Step 5 Configure alarm schedule and linkage.

Figure 5-163 Schedule and alarm linkage

1. Click .
2. Click **Setting** next to **Schedule** to configure the alarm period.

   The system performs linkage actions only for alarms during the arming period.

   - On the time line, drag to set the period.
   - You can also click to set the period.
3. Configure alarm linkage. For details, see Table 5-50 .

4. Click **Apply**.

Step 6 Click **Apply**.

5.9.8.2.5 People Stay Detection

When the target stays in the detection area longer than the defined duration, an alarm will be triggered.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Stereo Analysis**.

Step 2 Select a channel and then click **Add**.

Step 3 Select **Enable** and then set **Type** to **People Stay Detection**.

Step 4 Draw detection rule.

1. Click , and then draw a detection area on the video image. Right-click the image to stop drawing.
2. Configure parameters.

Table 5-45 Parameters of people stay detection

Parameter	Description
Name	Customize the rule name.
Sensitivity	Set alarm sensitivity.
Duration	Set low long people stay in the detection area until an alarm is triggered.
Repeat Alarm Time	Set repeat alarm time. If the alarm-triggering event continues, an alarm will be triggered again when repeat alarm time passed.

3. Click **OK**.

Step 5 Configure alarm schedule and linkage.

Figure 5-164 Schedule and alarm linkage

1. Click .
2. Click **Setting** next to **Schedule** to configure the alarm period.

   The system performs linkage actions only for alarms during the arming period.

   - On the time line, drag to set the period.
   - You can also click to set the period.

3. Configure alarm linkage. For details, see Table 5-50 .
4. Click **Apply**.

Step 6 Click **Apply**.

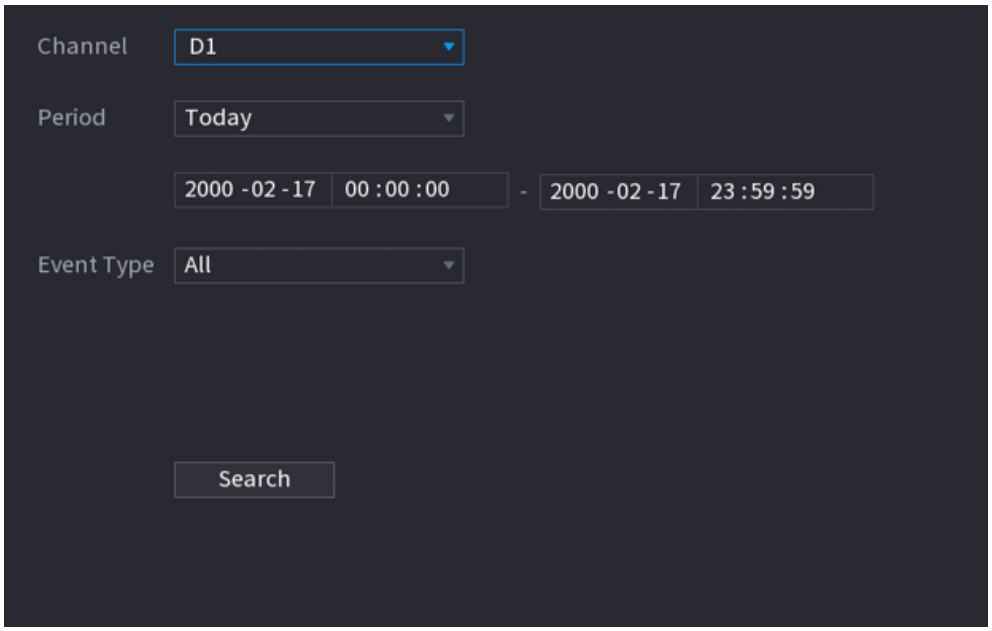
5.9.8.3 AI Search (Stereo Analysis)

You can search for detection results of stereo analysis.

Procedure

Step 1 Select **Main Menu** > **AI** > **AI Search** > **Stereo Analysis**.

Figure 5-165 Stereo analysis search



Step 2 Select a channel, start time, end time, event type, and then click **Search**.

The search results are displayed.

Related Operations

- Play back video.

  Click an image, and then click to play back the related video.

  During playback, you can:

  - Click to pause.
  - Click to stop.
  - Click to display AI rule. The icon changes to .
- Add tags.

  Select one or more images, and then click **Add Tag**.
- Lock.

  Select one or more images, and then click **Lock**. The locked files will not be overwritten.
- Export.

  Select one or more images, and then click **Export** to export selected search results in excel.
- Back up.

  Select one or more images, click **Backup** , select the storage path and file type, and then click **Start** to export files to external storage device.

5.9.9 Video Metadata

The system analyzes real-time video stream to detect the existence of human, motor vehicle, and non-motor vehicle. Once a target is detected, an alarm is triggered.

5.9.9.1 Enabling Smart Plan

To use AI by camera, you need to enable the smart plan first. For details, see "5.9.3 Smart Plan".

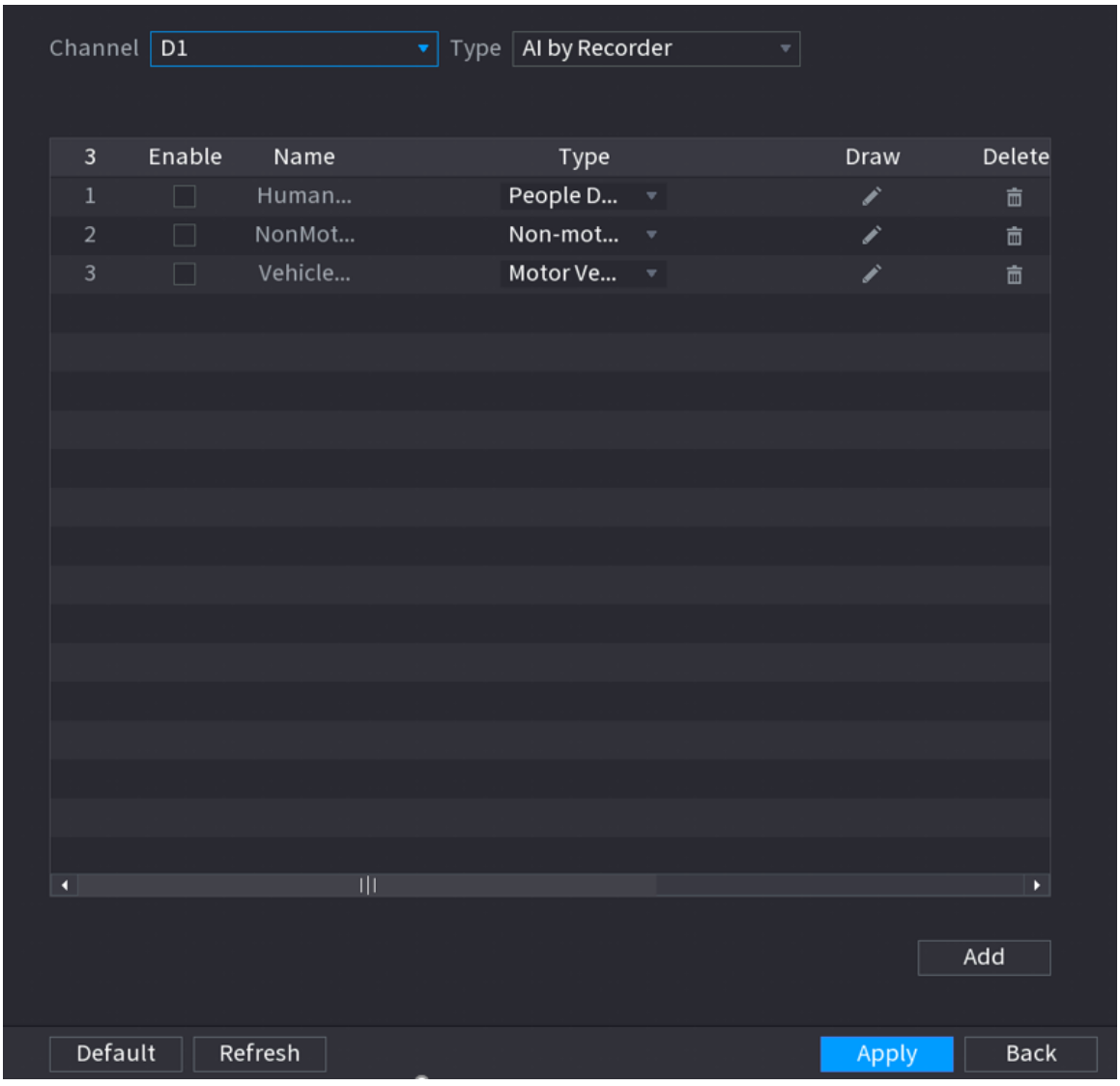
5.9.9.2 Configuring Video Metadata

When a metadata alarm is triggered, the system links the corresponding camera to record videos and logs and take snapshots. Other alarm linkage actions are not supported for video metadata.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Video Metadata**.

Figure 5-166 Video metadata



Step 2 Select a channel and AI type.

AI by Recorder is available on select models.

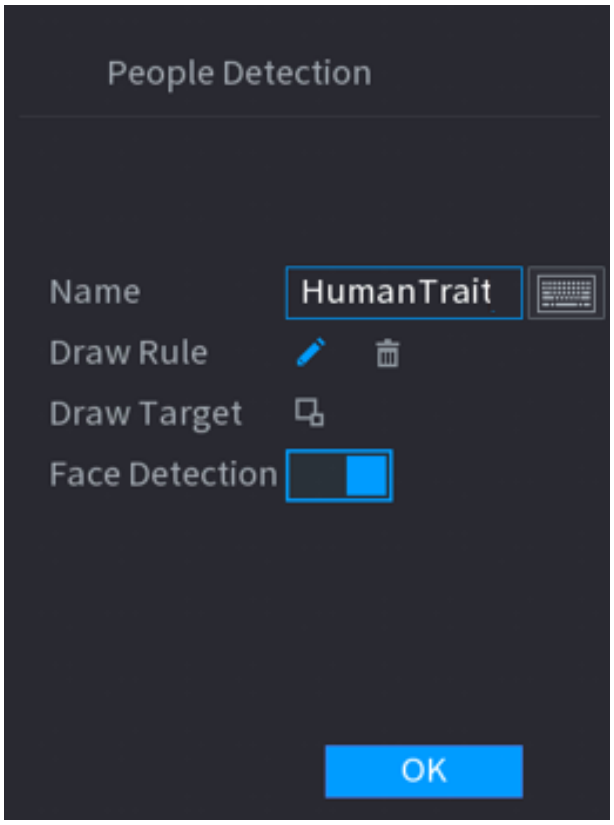
Step 3 Click **Add** to add a rule.

Step 4 Select **Enable** and then set **Type** to **People Detection**, **Non-motor Vehicle Detection** or **Motor Vehicle Detection**.

Step 5 Draw detection rule.

1. Click , and then draw a detection area on the video image. Right-click the image to stop drawing.

Figure 5-167 People detection



2. Enter the rule name.
3. Click to draw the minimum size or maximum size to filter the target.

   The system triggers an alarm only when the size of detected target is between the maximum size and the minimum size.
4. Click to enable face detection.
5. Select **A to B** , **B to A**, or **Both** as direction for tripwire counting.

   Tripwire counting is available when AI by Camera is used and the camera supports this function.
6. Click **OK**.

Step 6 Click **Apply**.

5.9.9.3 AI Search (Video Metadata)

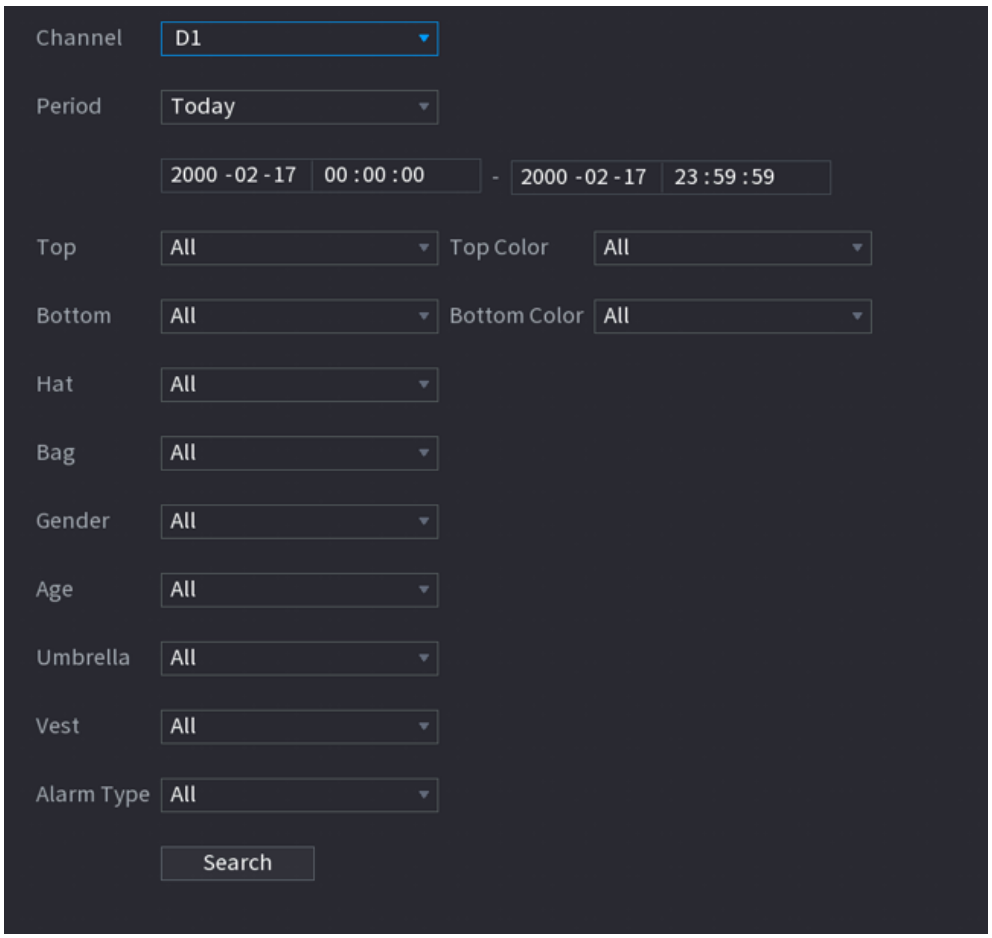
You can search for the video metadata detection results and play back related videos.

5.9.9.3.1 Human Detection

Procedure

Step 1 Select **Main Menu** > **AI** > **AI Search** > **Human Detection**.

Figure 5-168 Human detection

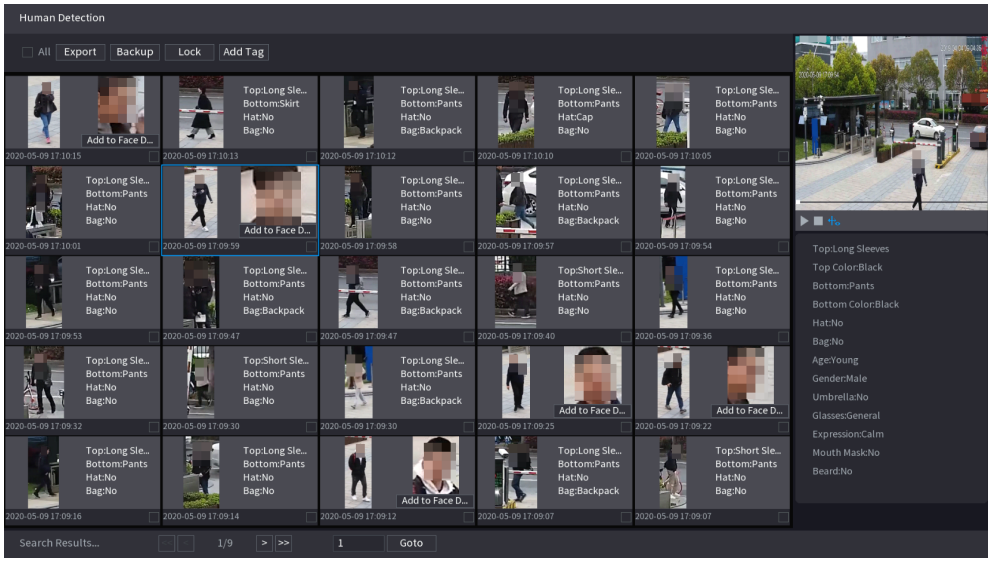


Step 2 Select a channel, start time, end time, and set corresponding parameters.

Step 3 Click **Search**.

For privacy protection, the faces are intentionally blurred.

Figure 5-169 Search results



Related Operations

- Play back video.

  Click an image, and then click to play back the related video.

  During playback, you can:

  - Click to pause.
  - Click to stop.
  - Click to display AI rule. The icon changes to .
- Add tags.

  Select one or more images, and then click **Add Tag**.
- Lock.

  Select one or more images, and then click **Lock**. The locked files will not be overwritten.
- Export.

  Select one or more images, and then click **Export** to export selected search results in excel.
- Back up.

  Select one or more images, click **Backup** , select the storage path and file type, and then click **Start** to export files to external storage device.

5.9.9.3.2 Motor Vehicle Detection

Background Information

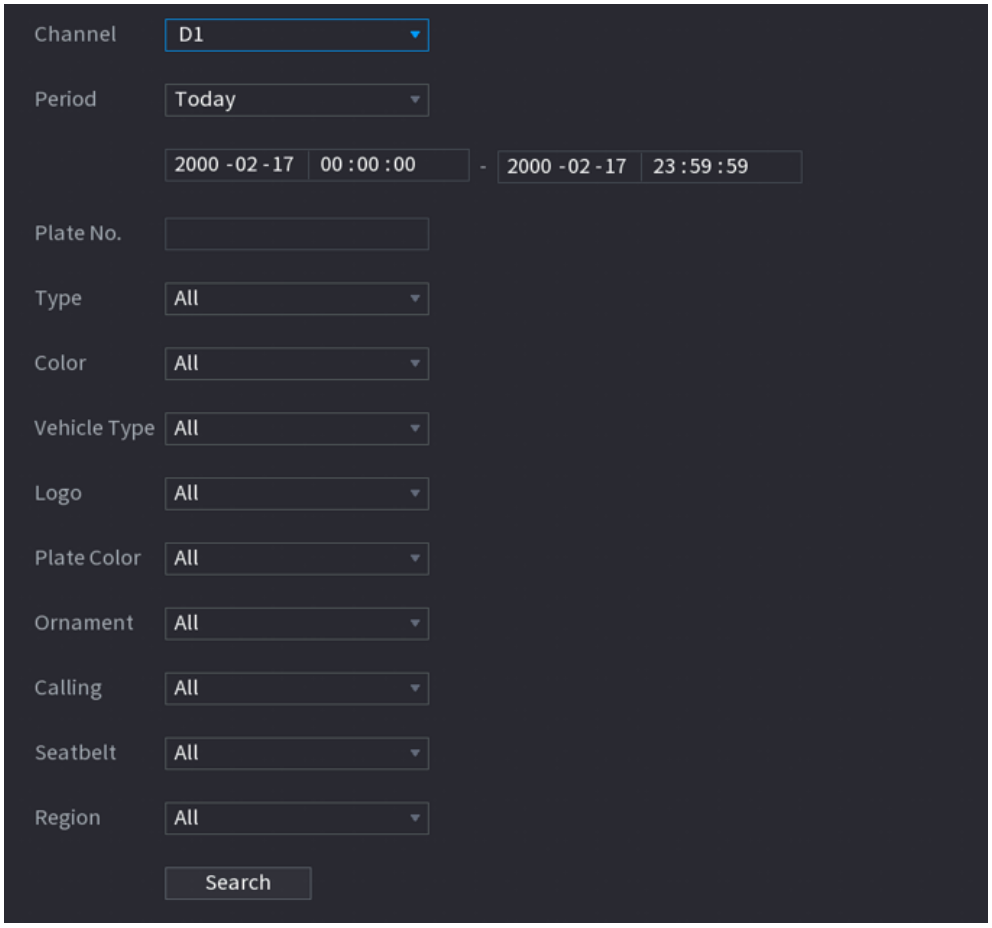
You can search for motor vehicle detection results according to the vehicle parameters.

This function is available on select models.

Procedure

Step 1 Select **Main Menu** > **AI** > **AI Search** > **Motor Vehicle Detection**.

Figure 5-170 Motor vehicle detection



Step 2 Select a channel and then set parameters.

- The system supports fuzzy search of plate numbers.
- The system searches all plate numbers by default if you have not set a plate number.

Step 3 Click **Search**.

The search results are displayed.

Related Operations

- Play back video.

  Click an image, and then click to play back the related video.

  During playback, you can:

  - Click to pause.
  - Click to stop.
  - Click to display AI rule. The icon changes to .
- Add tags.

  Select one or more images, and then click **Add Tag**.
- Lock.

  Select one or more images, and then click **Lock**. The locked files will not be overwritten.
- Export.

  Select one or more images, and then click **Export** to export selected search results in excel.

- Back up.

  Select one or more images, click **Backup** , select the storage path and file type, and then click **Start** to export files to external storage device.

5.9.9.3.3 Non-motor Vehicle Detection

Background Information

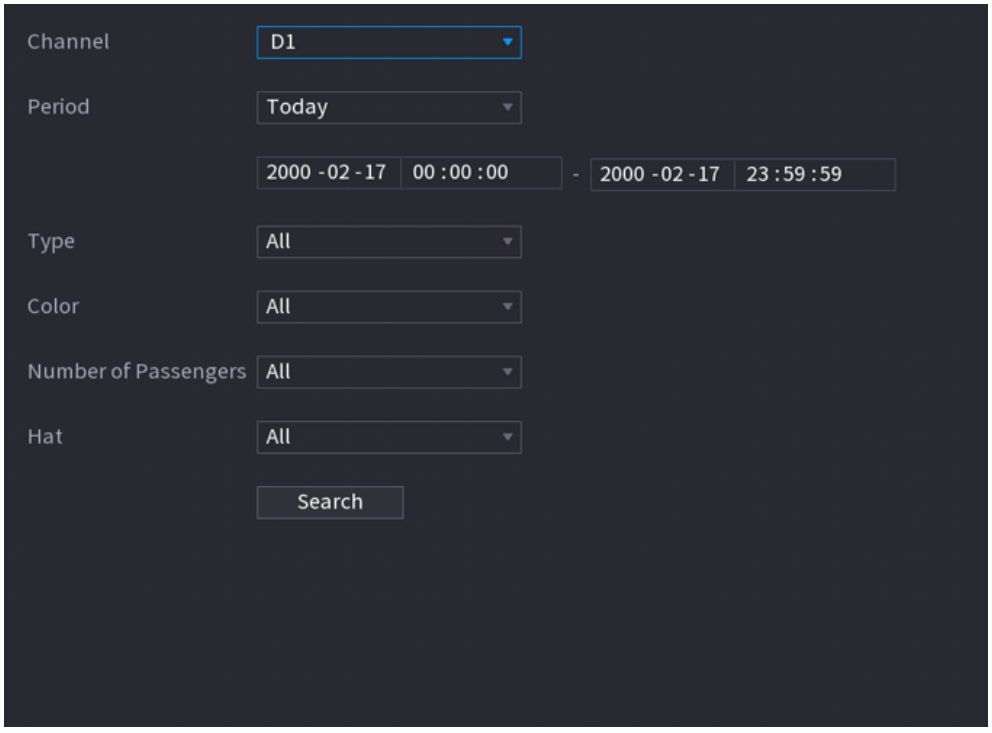
You can search for non-motor vehicle detection results according to the non-motor vehicle parameters.

This function is available on select models.

Procedure

Step 1 Select **Main Menu** > **AI** > **AI Search** > **Non-Motor Vehicle Detection** .

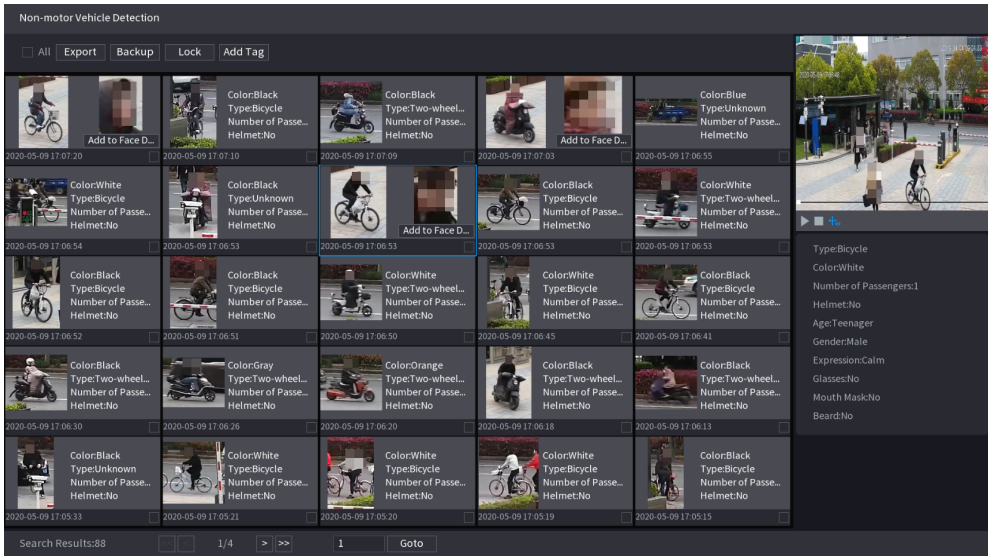
Figure 5-171 Non-motor vehicle detection



Step 2 Select a channel and then set parameters.

Step 3 Click **Search**.

Figure 5-172 Search results



Related Operations

- Play back video.

  Click an image, and then click to play back the related video.

  During playback, you can:

  - Click to pause.
  - Click to stop.
  - Click to display AI rule. The icon changes to .
- Add tags.

  Select one or more images, and then click **Add Tag**.
- Lock.

  Select one or more images, and then click **Lock**. The locked files will not be overwritten.
- Export.

  Select one or more images, and then click **Export** to export selected search results in excel.
- Back up.

  Select one or more images, click **Backup** , select the storage path and file type, and then click **Start** to export files to external storage device.

5.9.9.3.4 Report Query

Background Information

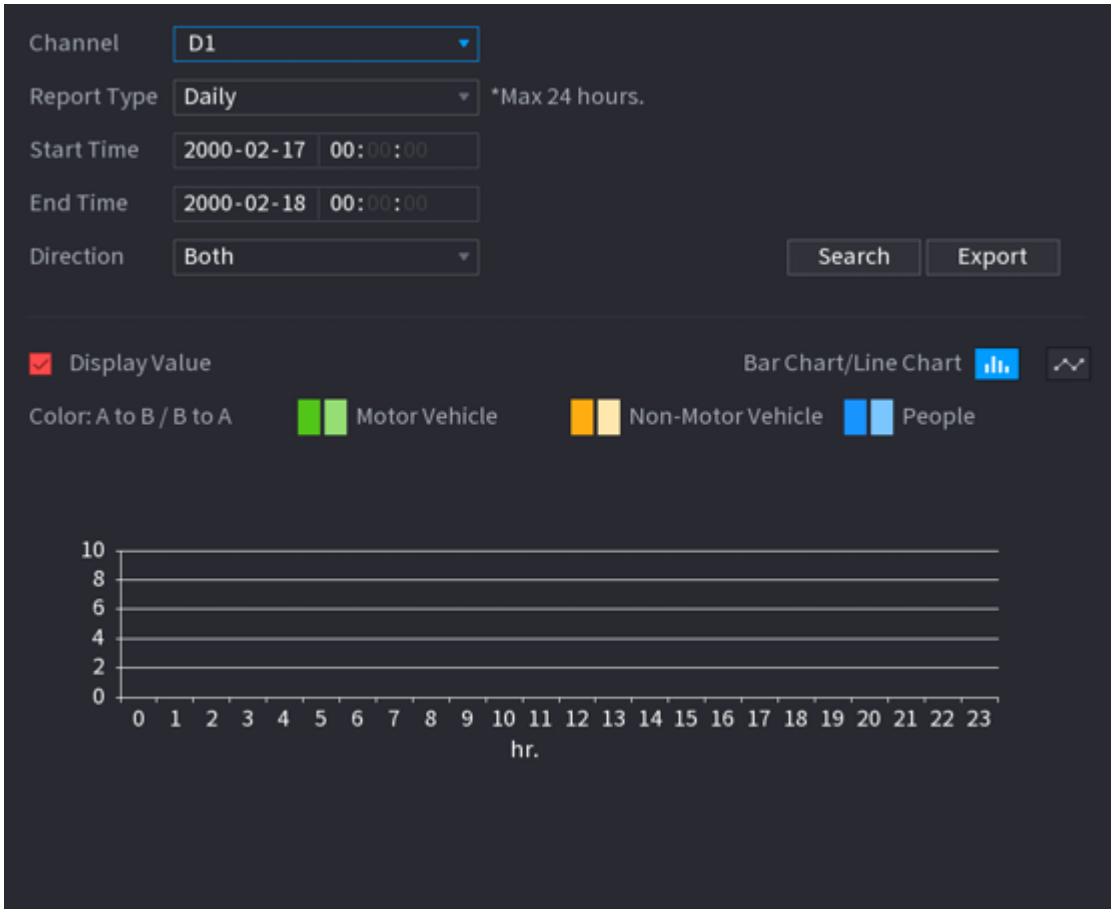
You can search for and export video metadata statistics.

- The statistics might be overwritten when the storage space runs out. Back up in time.
- When you restore the Device to factory settings, all the data except data in the external storage device will be cleared. You can clear the data in the external storage device through formatting or other methods.

Procedure

Step 1 Select **Main Menu** > **AI** > **Report Query** > **Video Metadata**.

Figure 5-173 Metadata statistics



Step 2 Select channel, report type, start time and end time, direction and then click **Search**.

Related Operations

- Switch chart type.

  Click **Bart Chart** or **Line Chart** to switch the chart type.
- Export.

  Select file type, and then click **Export** to export the report in picture or csv format.

5.9.10 ANPR

The system extracts the plate number on the surveillance video and then compare it with the specified plate information. When a match is detected, the system triggers an alarm.

5.9.10.1 Adding Vehicle Blocklist and Allowlist

Background Information

To facilitate vehicle management, you can add the plate numbers to the blocklist or allowlist. The system can compare the detected plate information with the plate on the blocklist and allowlist and then trigger the corresponding alarm linkage.

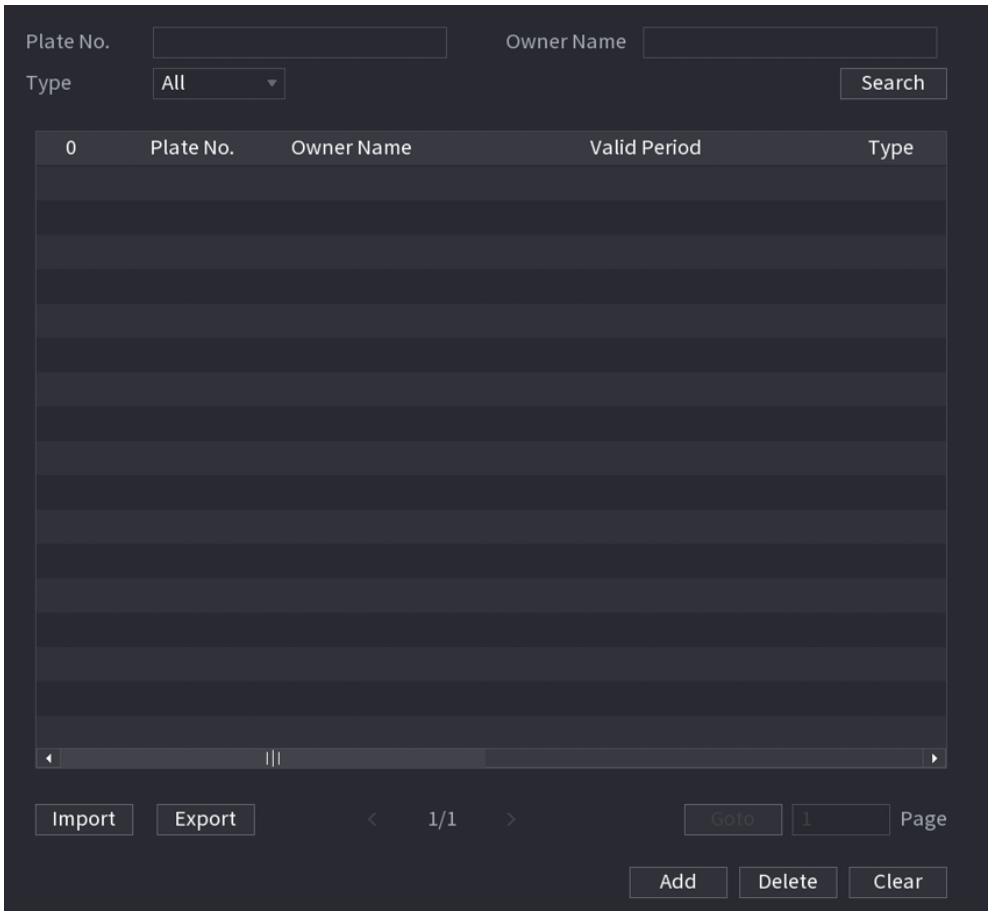
- With the blocklist and allowlist enabled, on the live page, the plate on the blocklist is displayed as red on the plate list and the plate on the allowlist is displayed as green. For the plate not on the blocklist or allowlist, the color is white.

- The added blocklist and allowlist will be synchronized to the connected ITC camera.

Procedure

Step 1 Select **Main Menu** > **AI** > **Database** > **Vehicle Blocklist/Allowlist**.

Figure 5-174 Vehicle blocklist/allowlist



Step 2 Click **Add**.

Step 3 Set plate information such as plate number, car owner name, select **Block List** or **Allow List**, and then set validity period.

Step 4 Click **OK**.

Related Operations

- Search.

  Enter keywords for **Plate No.** and **Owner Name**, select type and then click **Search**.
- Import and export plate information.
  - Import: Click **Import** , select the corresponding file, and then click **Browse** to import the file.
  - Export: Click **Export** , select the file storage path and then click **Save**.
- Delete plate information.
  - Delete one by one: Click the of the corresponding plate number.
  - Delete in batches: Select the plate numbers and then click **Delete**.

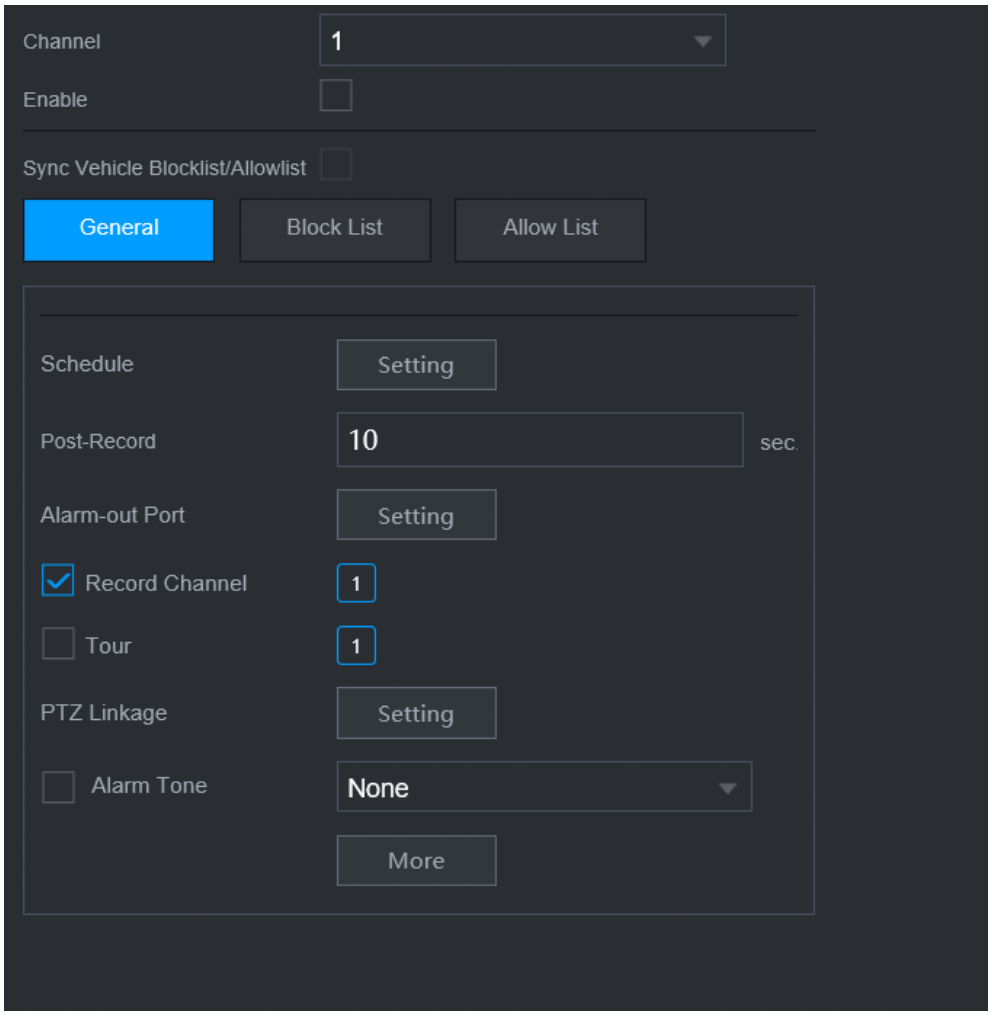
5.9.10.2 Configuring ANPR

Configure the ANPR alarm rules.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameters** > **ANPR**.

Figure 5-175 ANPR



Step 2 Select a channel and then select the **Enable** checkbox to enable ANPR.

Step 3 (Optional) Enable **Sync Vehicle Blocklist/Allowlist** to synchronize the blocklist and allowlist on the NVR to the connected camera.

Step 4 Click **General** (default), **Blocklist** or **Allowlist** tab.

Before enabling the blocklist alarm or allowlist alarm, you need to add the corresponding plate information.

- **General** : The system triggers an alarm when it detects any plate number.
- **Block List** : The system triggers an alarm when it detects plate number on the blocklist.
- **Allow List** : The system triggers an alarm when it detects plate number on the allowlist.

Step 5 Click **Setting** next to **Schedule** to configure the arming period.

The system triggers corresponding alarm actions only during the arming period.

- On the time line, drag to set the period.
- You can also click to set the period.

Step 6 Configure alarm linkage actions. For details, see Table 5-50 .

Step 7 Click **Apply**.

5.9.10.3 AI Search (ANPR)

You can search for the ANPR detection results. For details, see "5.9.9.3.2 Motor Vehicle Detection".

5.9.11 Crowd Distribution

The system detects the crowd distribution. When the crowd density exceeds the defined threshold, an alarm is triggered.

5.9.11.1 Enabling Smart Plan

To use AI by camera, you need to enable the smart plan first. For details, see "5.9.3 Smart Plan".

5.9.11.2 Configuring Crowd Distribution

Configure the alarm rules of crowd distribution detection.

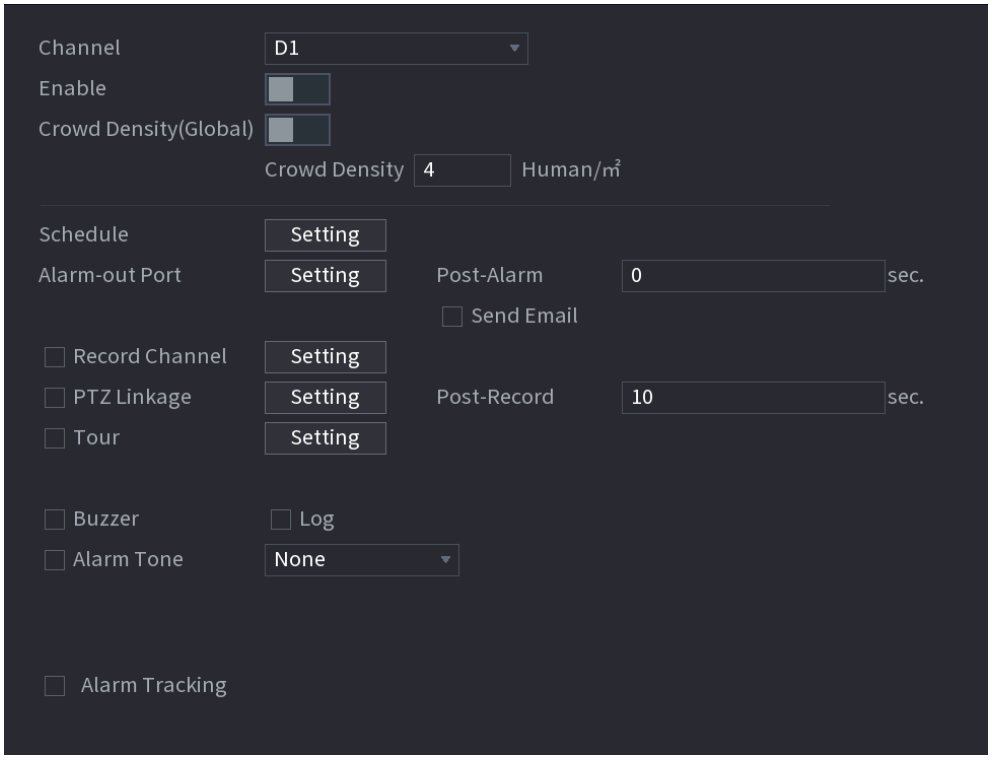
Prerequisites

Make sure that the connected camera supports the crowd distribution function.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameters** > **Crowd Distribution**.

Figure 5-176 Crowd distribution



Step 2 Select a channel and then click next to **Enable**.

Step 3 Configure parameters.

Table 5-46 Crowd distribution parameters

Parameter	Description
Crowd Density (Global)	Click and then configure the density threshold.
Crowd Density	
Alarm Tracking	After an alarm occurs, the system tracks the target automatically.

Step 4 Click **Setting** next to **Schedule** to configure the arming period.

The system triggers corresponding alarm actions only during the arming period.

- On the time line, drag to set the period.
- You can also click to set the period.

Step 5 Configure alarm linkage actions. For details, see Table 5-50 .

Step 6 Click **Apply**.

5.9.11.3 Report Query

Background Information

You can search for and export video metadata statistics.

- The statistics might be overwritten when the storage space runs out. Back up in time.

- When you restore the Device to factory settings, all the data except data in the external storage device will be cleared. You can clear the data in the external storage device through formatting or other methods.

Procedure

Step 1 Select **Main Menu** > **AI** > **Report Query** > **Crowd Density**.

Step 2 Select the channel, report type, start time and end time, and then click **Search**.

Related Operations

- Switch chart type.

  Click **Bart Chart** or **Line Chart** to switch the chart type.
- Export.

  Select the file type, and then click **Export** to export the report in picture or csv format.

5.9.12 People Counting

The system can calculate the number of entry or exit people in the detection zone. An alarm is triggered when the number has exceeded the threshold.

Make sure that the connected camera supports people counting.

5.9.12.1 Enabling Smart Plan

To use AI by camera, you need to enable the smart plan first. For details, see "5.9.3 Smart Plan".

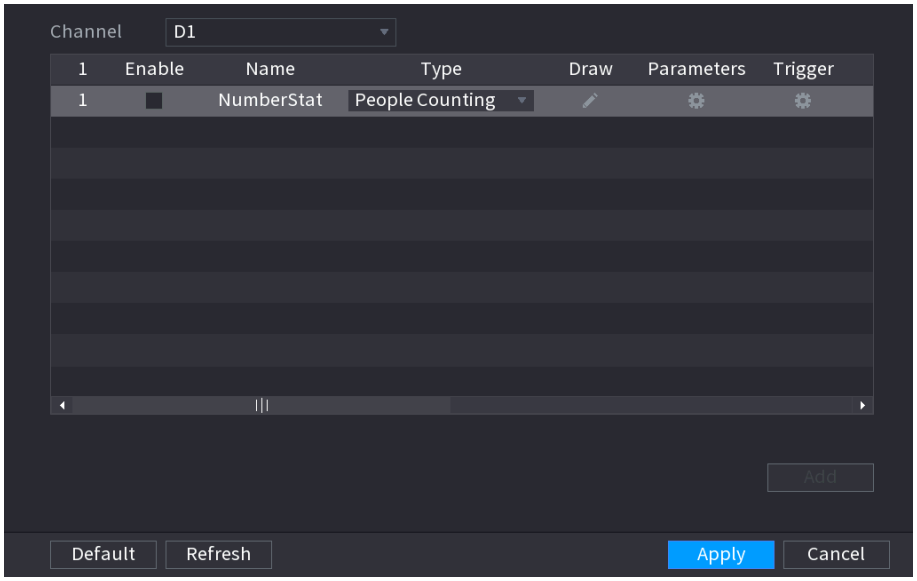
5.9.12.2 Configuring People Counting

The system counts the number of people in and out of the detection area. When the number of entry, exit or staying people exceeds the threshold, an alarm is triggered.

Procedure

Step 1 Select **Main Menu** > **AI** > **Parameters** > **People Counting** > **People Counting**.

Figure 5-177 People counting



Step 2 Select a channel, and then click **Add**.

Step 3 Select the **Enable** checkbox, and then set **Type** to **People Counting**.

Step 4 Draw people counting rule.

1. Click to draw the people counting rule. Right-click the image to stop drawing.
   - Press and hold the vertex of the rule line to adjust the size of the rule line.
   - Click to delete the drawn rule line.

Table 5-47 Relationship between rule and people counting

Rule	People Counting Type
Drawing detection area.	Count the number of people staying in the area.
Draw rule lines within the detection area and detection area separately. You can draw polylines for the tripwire, supporting up to 20 vertices.	Count the number of people crossing the rule lines within the detection area, such as the number of people entering, leaving, and passing.

2. Click to draw a target filtering area on the image.

Figure 5-248 Disk Quota

Step 2 (Optional) If **Disk group mode selected** is shown on the page, click **Switch to Quota Mode** and then follow the on-screen instructions to format disks.

Step 3 Select a channel and set the record duration, bit rate and storage capacity of picture.

Step 4 Click **Apply**.

5.12.6 Disk Check

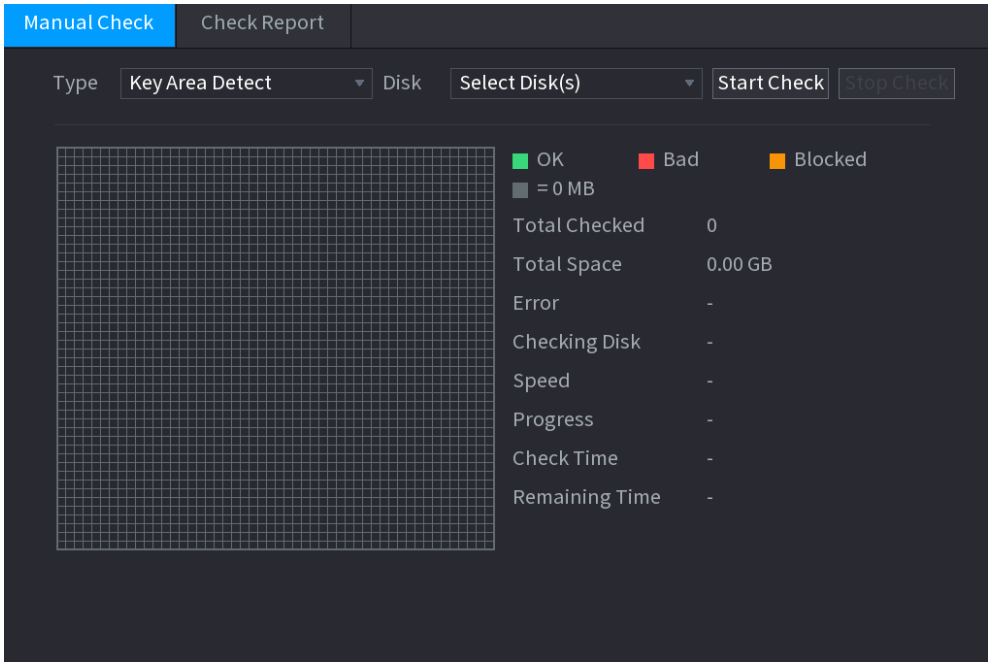
The system can detect HDD status so that you can clearly understand the HDD performance and replace the malfunctioning HDD.

5.12.6.1 Manual Check

Procedure

Step 1 Select **Main Menu** > **STORAGE** > **Disk Check** > **Manual Check**.

Figure 5-249 Manual check



Step 2 Select the detection type.

- Key area detect: The system detects the used space of the HDD through the built-in file system. This type of detection is efficient.
- Global detection: The system detects the entire HDD through Window. This type of detection takes time and might affect the HDD that is recording.

Step 3 Select the HDD that you want to detect.

Step 4 Click **Start Check**.

The system starts detecting the HDD and displays the detection information.

When system is detecting HDD, click **Stop Check** to stop current detection. Click **Start Check** to detect again.

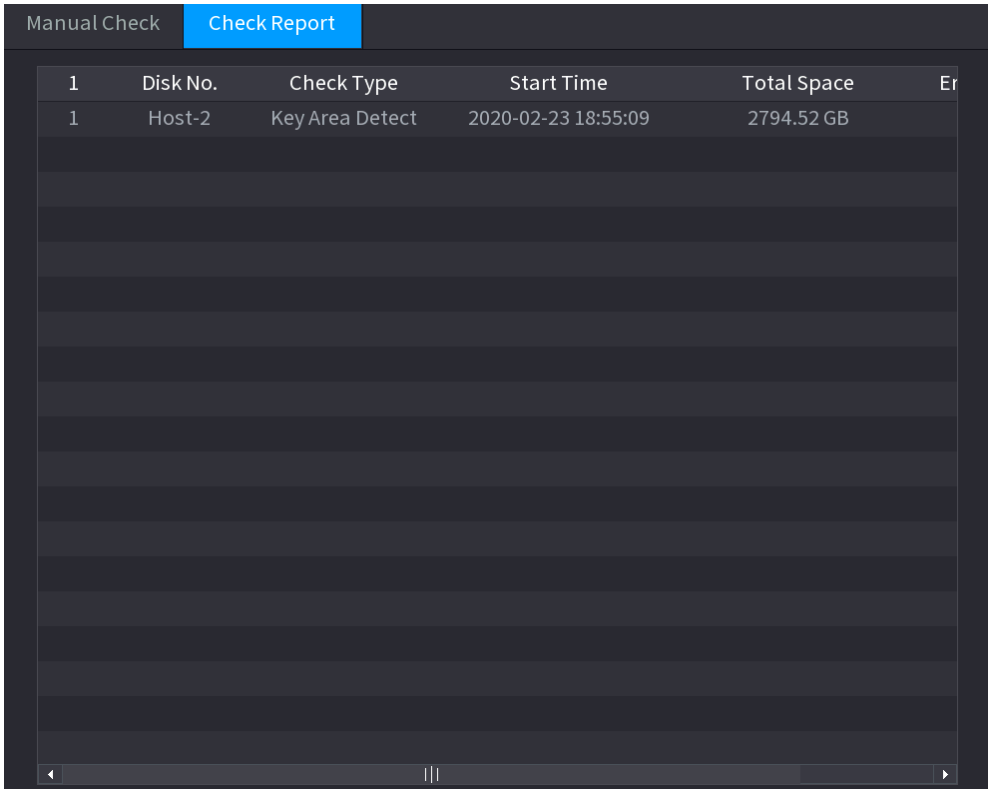
5.12.6.2 Detection Report

After the detection, you can view the detection report.

Procedure

Step 1 Select **Main Menu** > **STORAGE** > **Disk Check** > **Check Report**.

Figure 5-250 Check report



Step 2 Click to view detection results and S.M.A.R.T report.

Figure 5-251 Results

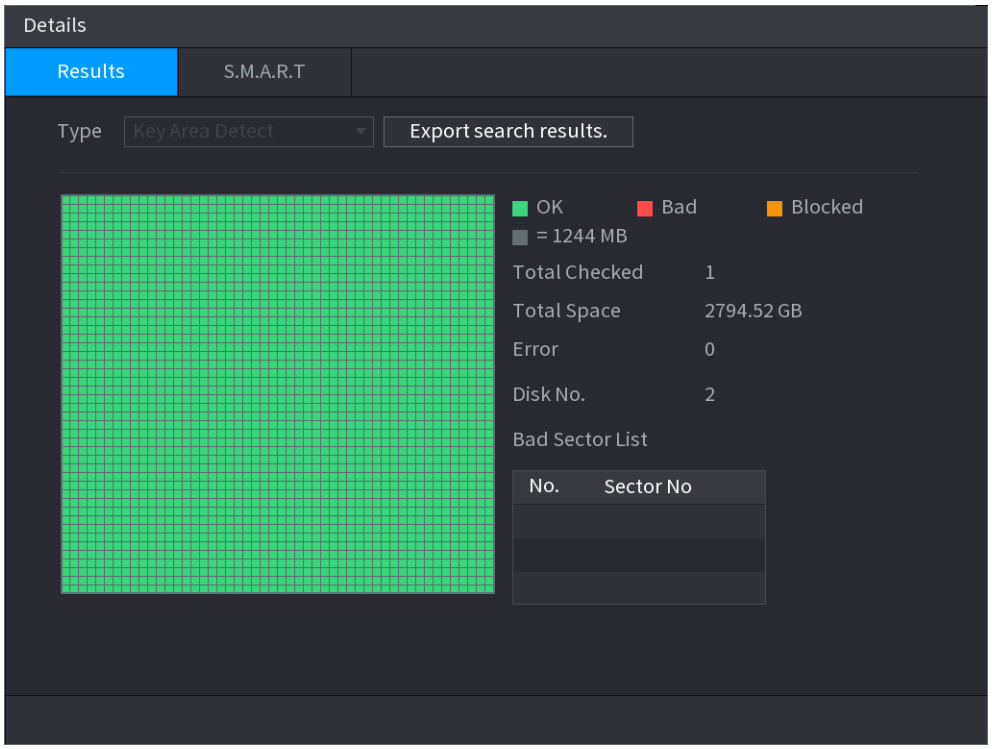
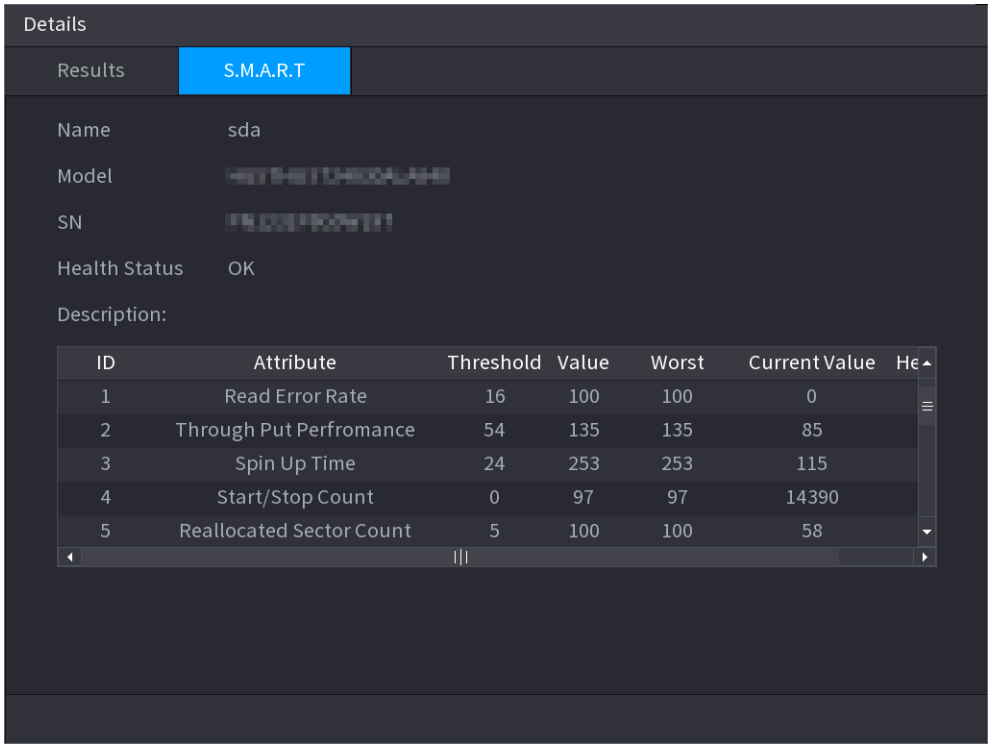


Figure 5-252 S.M.A.R.T



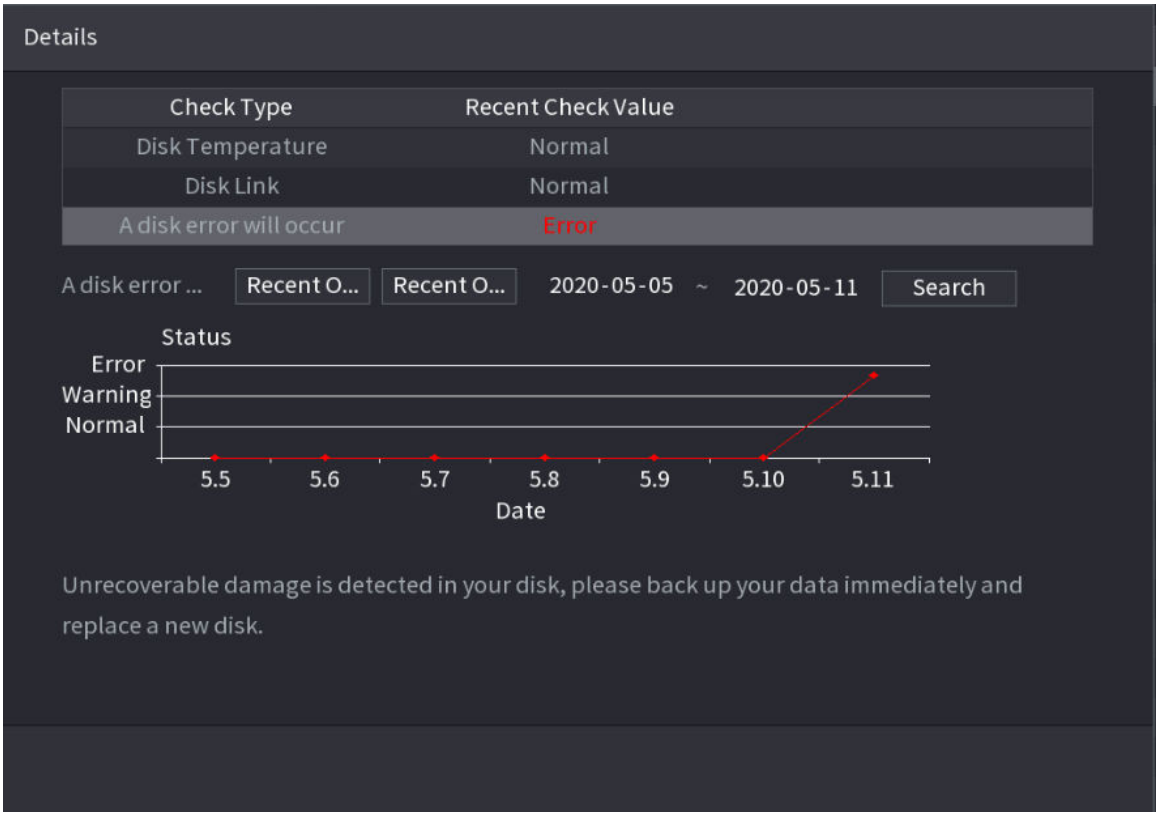
5.12.6.3 Disk Health Monitoring

Monitor health status of disks, and repair if any exceptions are found so as to avoid data loss.

Select **Main Menu** > **STORAGE** > **Disk Check** > **Health Monitoring**.

Click to show disk details page. Then select **Check Type** , set time period, and then click **Search**. The system shows the details of disk monitoring status.

Figure 5-253 Disk details



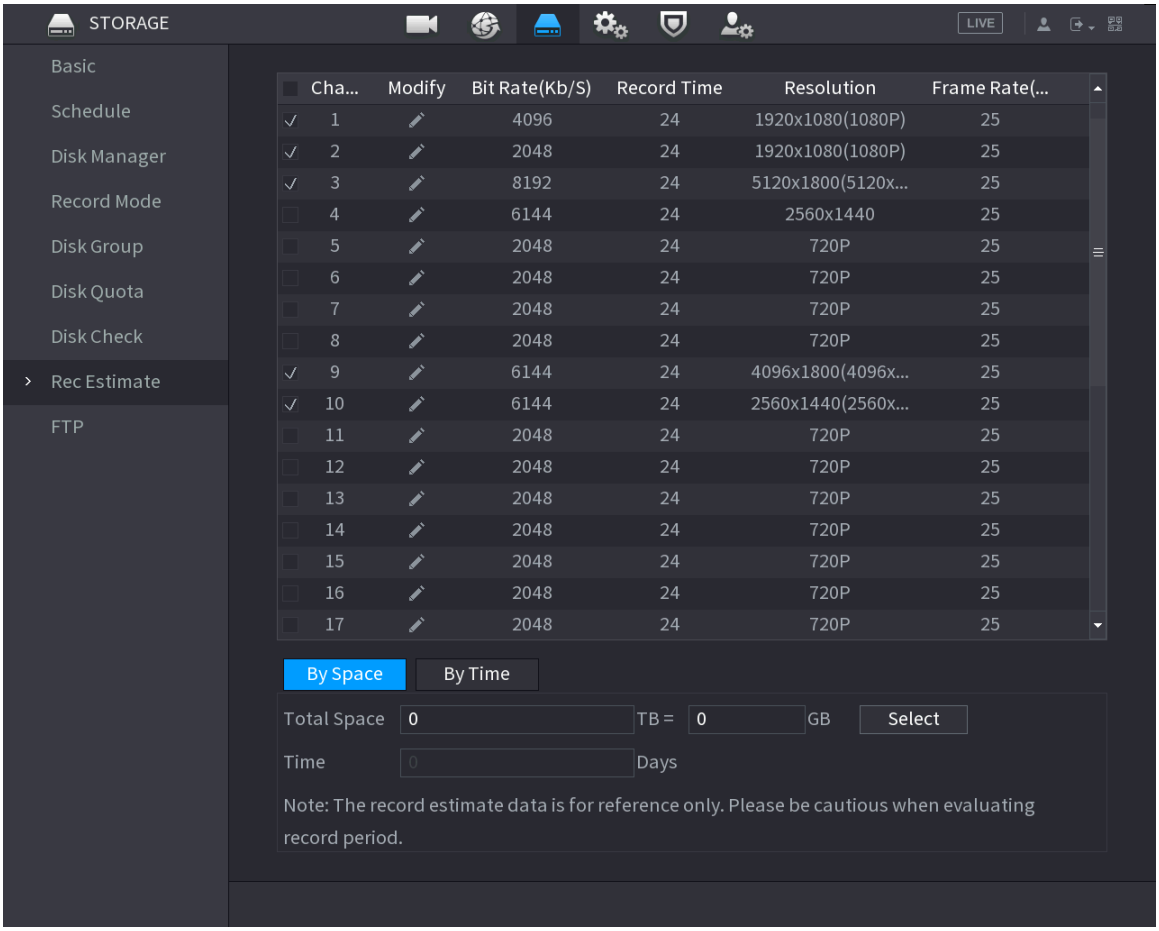
5.12.7 Record Estimate

Record estimate function can calculate how long you can record video according to the HDD capacity, and calculate the required HDD capacity according to the record period.

Procedure

Step 1 **Select Main Menu** > **STORAGE** > **Rec Estimate**.

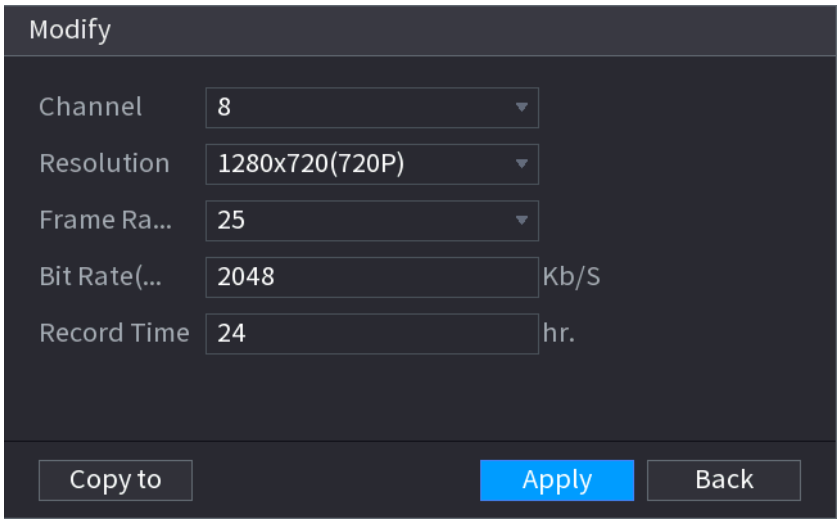
Figure 5-254 Record estimation



Step 2 Click .

You can configure the **Resolution** , **Frame Rate**, **Bit Rate** and **Record Time** for the selected channel.

Figure 5-255 Modify channel settings



Step 3 Click **Apply**.

Then the system will calculate the time period that can be used for storage according to the channels settings and HDD capacity.

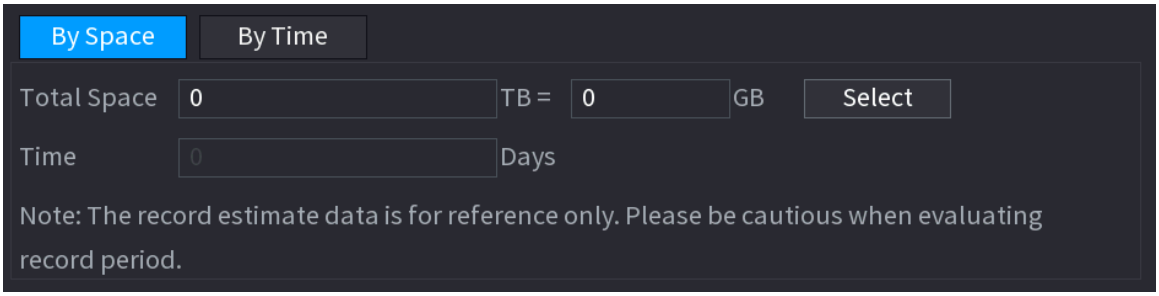
Click **Copy to** to copy the settings to other channels.

5.12.7.1 Calculating Recording Time

Procedure

Step 1 On the **Rec Estimate** page, click the **By Space** tab.

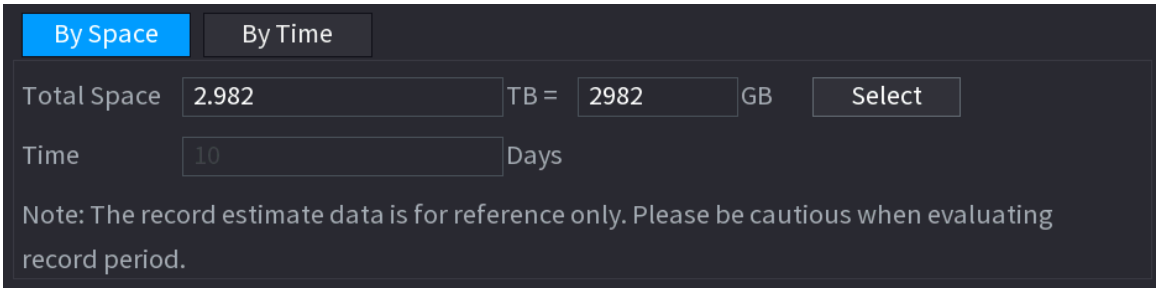
Figure 5-256 By space



Step 2 Click **Select**.

Step 3 Select the checkbox of the HDD that you want to calculate.

Figure 5-257 Recording time

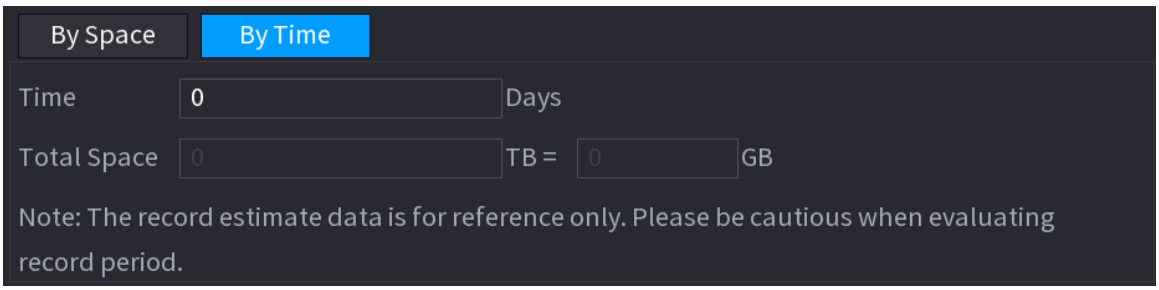


5.12.7.2 Calculating HDD Capacity for Storage

Procedure

Step 1 On the **Rec Estimate** page, click the **By Time** tab.

Figure 5-258 By time



Step 2 In the **Time** box, enter the time period that you want to record.

In the **Total Space** box, the required HDD capacity is displayed.

5.12.8 FTP

You can store and view the recorded videos and snapshots on the FTP server.

Prerequisites

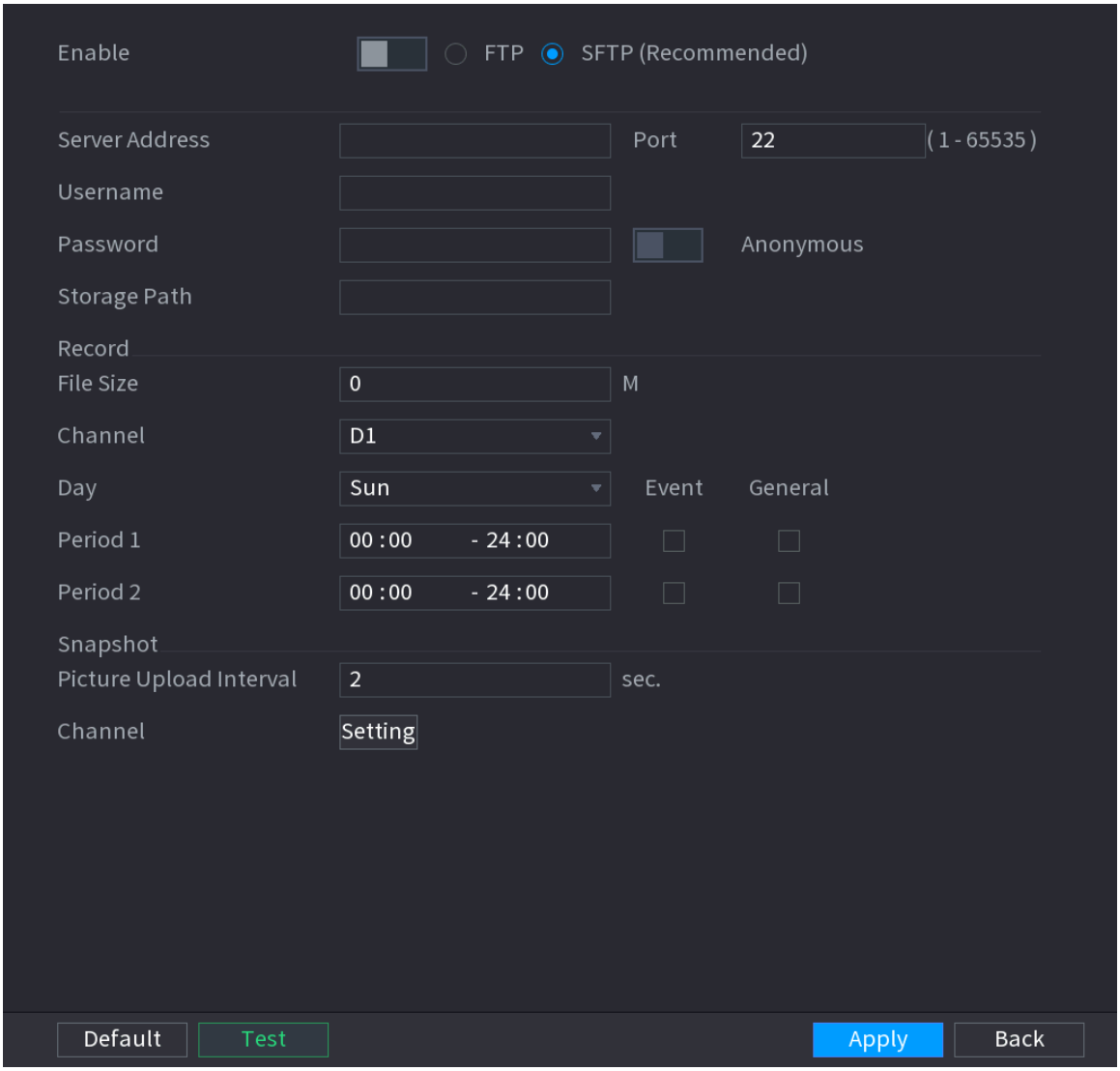
Purchase or download a FTP (File Transfer Protocol) server and install it on your PC.

For the created FTP user, you need to set the write permission; otherwise the upload of recorded videos and snapshots will be failed.

Procedure

Step 1 Select **Main Menu** > **STORAGE** > **FTP**.

Figure 5-259 FTP



Step 2 Configure the parameters.

Table 5-75 FTP parameters

Parameter	Description
Enable	Enable the FTP upload function.

Parameter	Description
FTP type	Select FTP type. ● FTP: Plaintext transmission. ● SFTP: Encrypted transmission (recommended).
Server Address	IP address of FTP server.
Port	Enter the port of the FTP server. ● FTP: The default is 21. ● SFTP: The default is 22.
Username	Enter the username and password to log in to the FTP server. If you enable the anonymity function, you can log in anonymously without entering the username and password.
Password	
Anonymous	
Storage Path	Create folder on FTP server. ● If you do not enter the name of remote directory, the system automatically creates the folders according to the IP and time. ● If you enter the name of remote directory, the system creates the folder with the entered name under the FTP root directory first, and then automatically creates the folders according to the IP and time.
File Size	Enter the length of the uploaded recorded video. ● If the entered length is less than the recorded video length, only a section of the recorded video can be uploaded. ● If the entered length is more than the recorded video length, the whole recorded video can be uploaded. ● If the entered length is 0, the whole recorded video will be uploaded.
Picture Upload Interval	● If this interval is longer than snapshot interval, the system takes the recent snapshot to upload. For example, the interval is 5 seconds, and snapshot interval is 2 seconds per snapshot, the system uploads the recent snapshot every 5 seconds. ● If this interval is shorter than snapshot interval, the system uploads the snapshot per the snapshot interval. For example, the interval is 5 seconds, and snapshot interval is 10 seconds per snapshot, the system uploads the snapshot every 10 seconds. ● To configure the snapshot interval, go to **Main Menu** > **CAMERA** > **Encode** > **Snapshot**.
Channel	Select the channel that you want to apply the FTP settings.
Day	Select the week day and set the time period that you want to upload the recorded files. You can set two periods for each week day.
Period 1, Period 2	
Record type	Select the record type (Alarm, Intel, MD, and General) that you want to upload. The selected record type will be uploaded during the configured time period.

Step 3 Click **Test** to validate the FTP connection.

If FTP connection failed, check the network and FTP settings.

Step 4 Click **Apply**.

5.12.9 iSCSI

Background Information

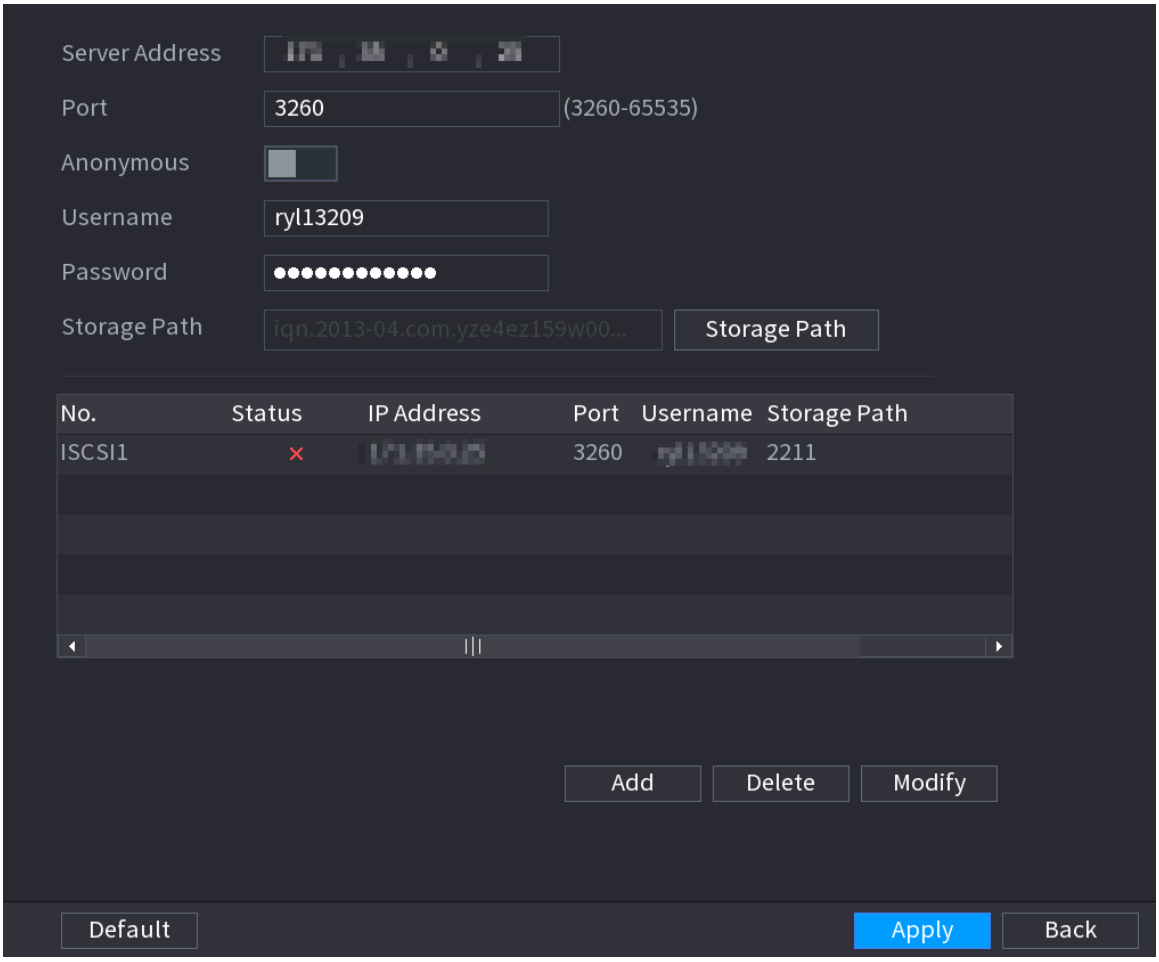
Internet Small Computer Systems Page (iSCSI) is a transport layer protocol that works on top of the Transport Control Protocol (TCP), and enables block-level SCSI data transport between the iSCSI initiator and the storage target over TCP/IP networks. After the network disk is mapped to the NVR device through iSCSI, the data can be stored on the network disk.

This function is available on select models.

Procedure

Step 1 Select **Main Menu** > **STORAGE** > **iSCSI**.

Figure 5-260 iSCSI



Step 2 Set parameters.

Table 5-76 iSCSI parameters

Parameter	Description
Server Address	Enter the server address of iSCSI server.
Port	Enter the port of iSCSI server, and the default value is 3260.

Parameter	Description
Storage Path	Click **Storage Path** to select a remote storage path. Each path represents an iSCSI shared disk and these paths are generated when created on the server.
Username, Password	Enter the username and password of iSCSI server. If anonymous login is supported by iSCSI server, you can enable **Anonymous** to log in as an anonymous user.

Step 3 Click **Apply**.

5.13 Account

You can manage users, user group and ONVIF user, and set admin security questions.

5.13.1 Group

The accounts of the Device adopt two-level management mode: user and user group. Every user must belong to a group, and one user only belongs to one group.

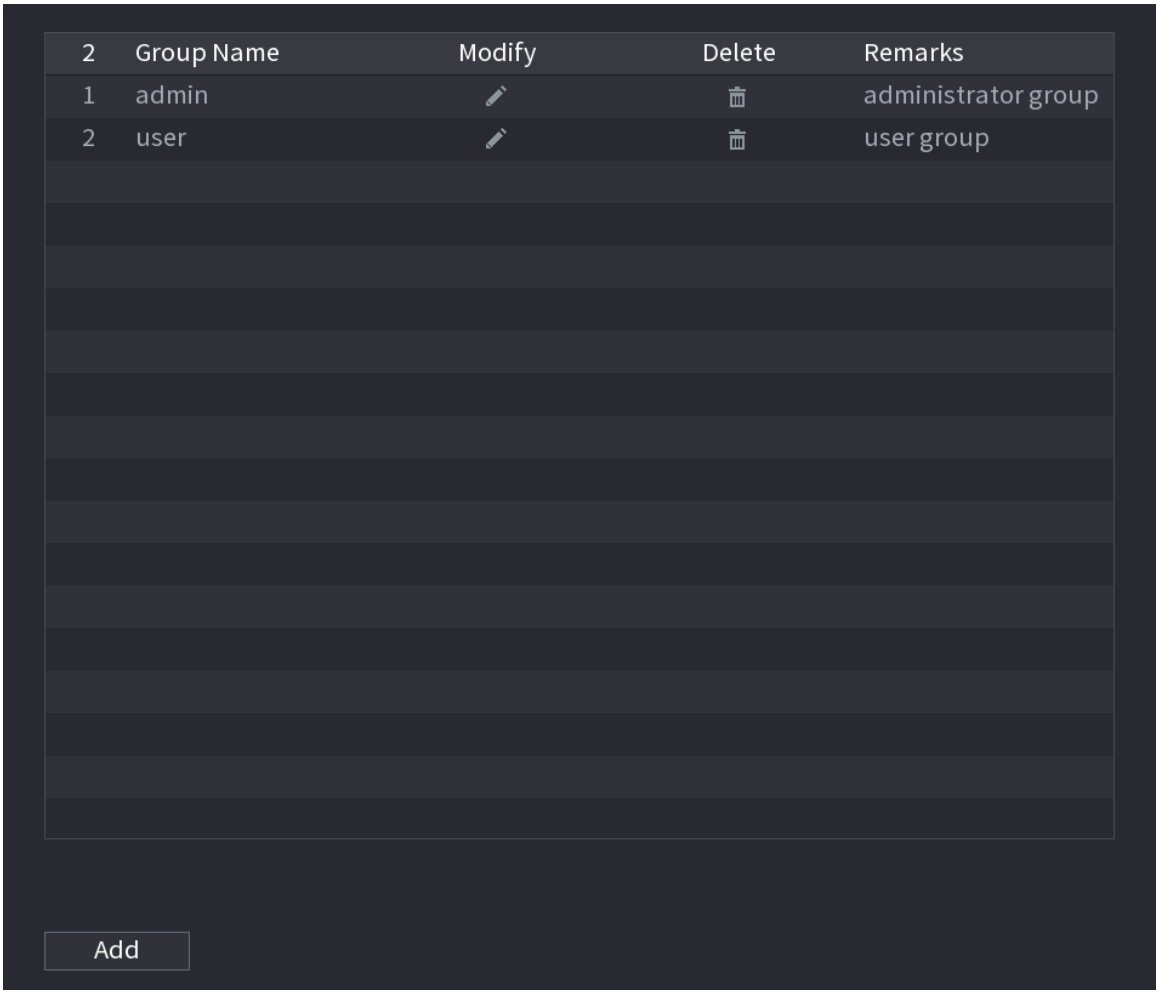
Background Information

The **admin** and **user** group are two default user groups that cannot be deleted. You can add more groups and define corresponding permissions.

Procedure

Step 1 Select **Main Menu** > **ACCOUNT** > **Group**.

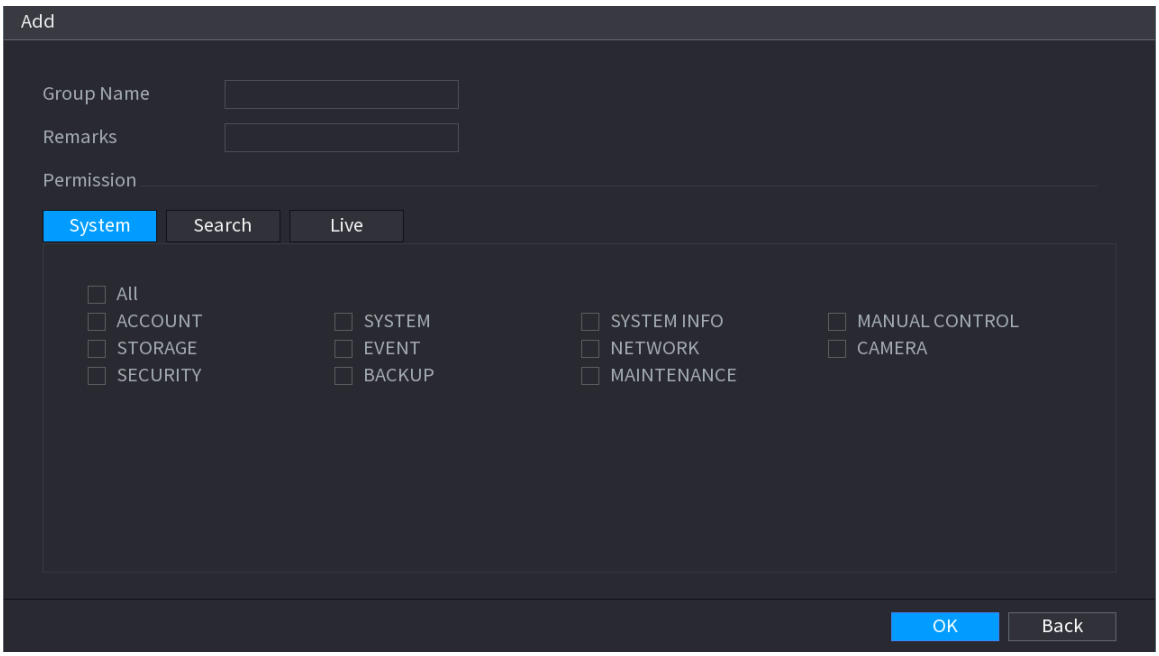
Figure 5-261 Group



Step 2 Click **Add**.

Step 3 Enter group name and then enter some remarks if necessary.

Figure 5-262 Add group



Step 4 Select the checkboxes to select permissions.

Step 5 Click **OK**.

Click to modify the corresponding group information, click to delete the group.

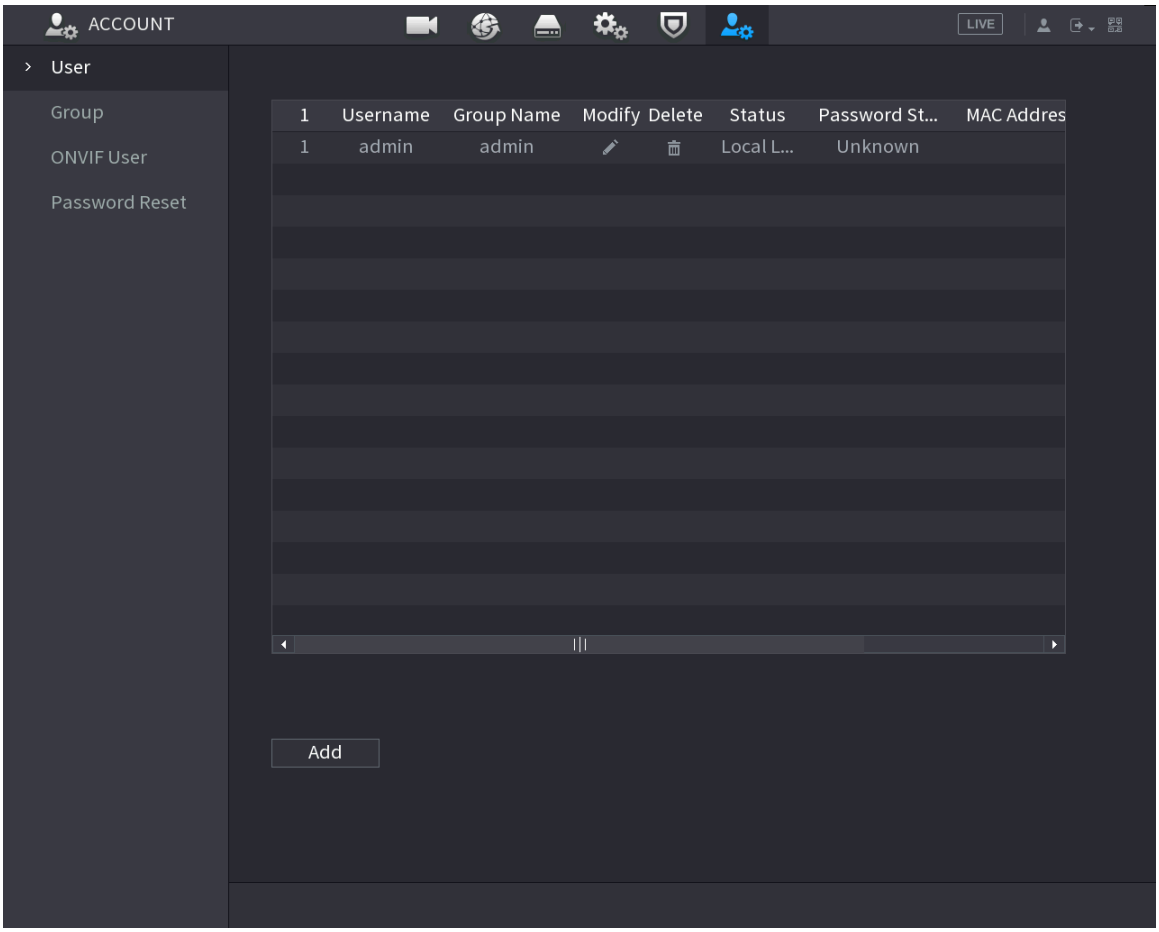
5.13.2 User

5.13.2.1 Adding User

Procedure

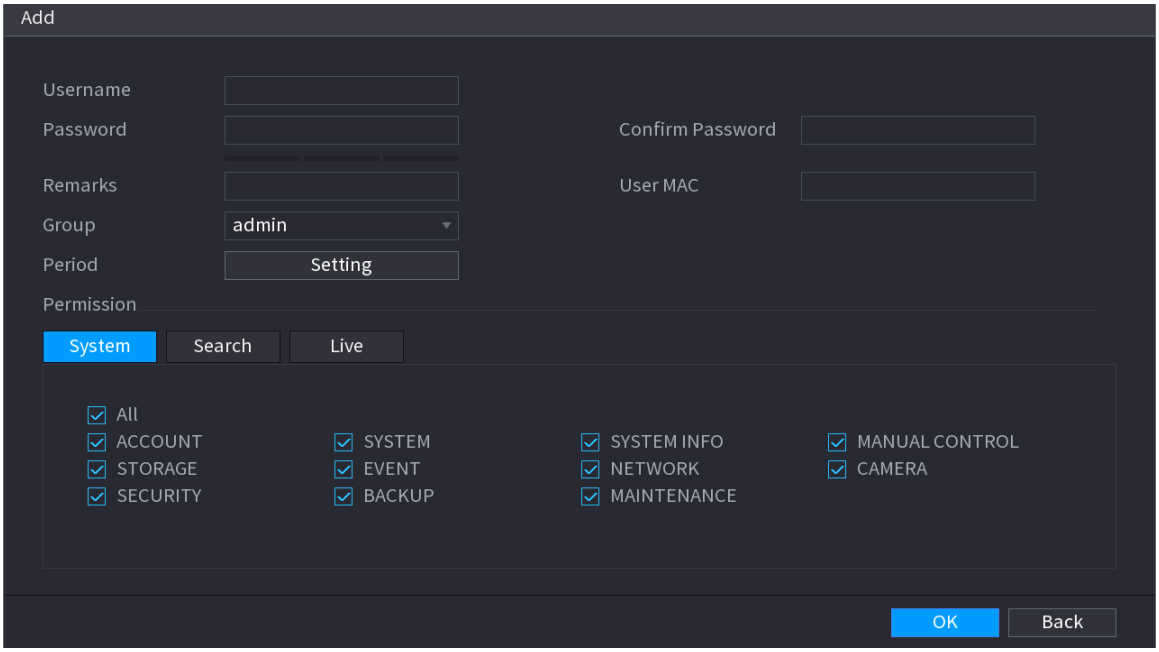
Step 1 Select **Main Menu** > **ACCOUNT** > **User**.

Figure 5-263 User



Step 2 Click **Add**.

Figure 5-264 Add user



Step 3 Configure the parameters.

Table 5-77 Parameters of adding user

Parameter	Description
Username	Enter a username and password for the account.
Password	
Confirm Password	Enter the password again to confirm it.
Remarks	Optional. Enter a description of the account.
User MAC	Enter user MAC address
Group	Select a group for the account. The user rights must be within the group permissions.
Period	Click **Setting** to define a period during which the new account can log in to the Device. The new account cannot access the device during other periods.
Permission	Select the checkboxes to grant permissions to the user. To manage the user account easily, when defining the user account permission, do not give the authority to the common user account higher that the advanced user account.

Step 4 Click **OK**.

Click to modify the corresponding user information, click to delete the user.

5.13.2.2 Changing Password

Background Information

We recommend you change the password regularly to enhance device security.

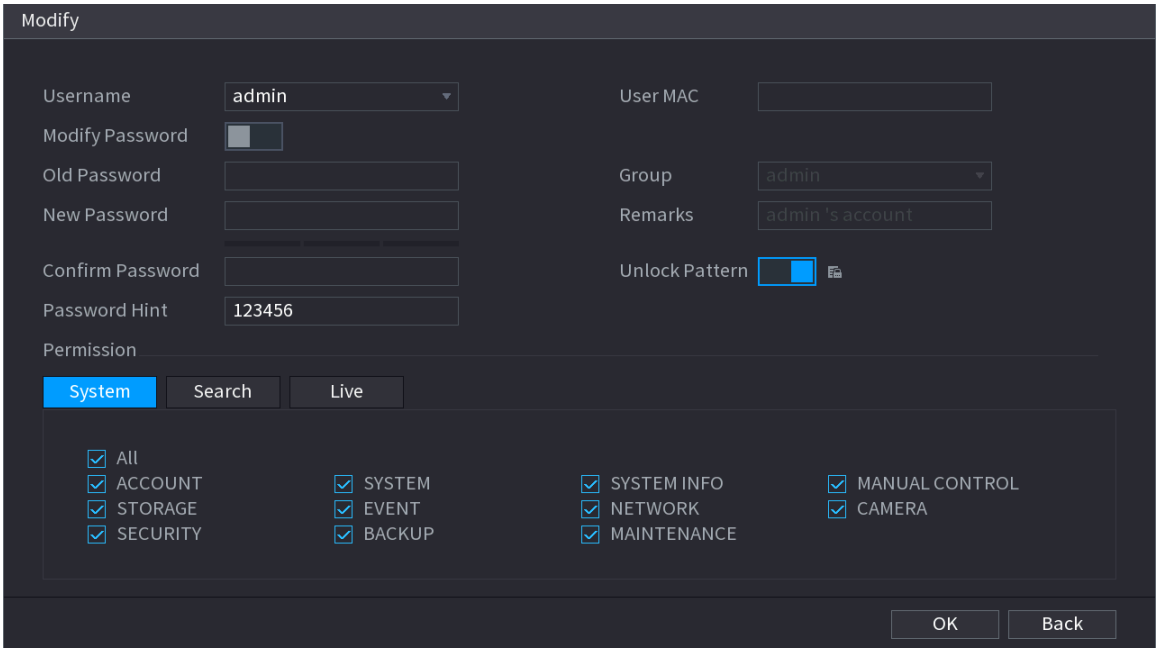
Users with account permissions can change the password of other users.

Procedure

Step 1 Select **Main Menu** > **ACCOUNT** > **User**.

Step 2 Click of the corresponding user.

Figure 5-265 Change password



Step 3 Click to enable the **Modify Password** function.

Step 4 Enter old password and then enter new password twice.

- The password must consist of 8–32 non-blank characters and contain at least two types of the following characters: uppercase, lowercase, numbers, and special characters (excluding ' " ; : &).
- For your device security, create a strong password.
- Check the box to enable Unlock Pattern function, click .

Step 5 Click to enable **Unlock Pattern** and then click to draw the pattern.

Step 6 Click **OK**.

5.13.3 Resetting Password

You can reset the password when you forget the password.

5.13.3.1 Enabling Password Reset

Enable the password reset function and configure the linked email address and security questions that are used to reset the password.

Procedure

Step 1 Select **Main Menu** > **ACCOUNT** > **Password Reset**.

Step 2 Click to enable the password reset function.

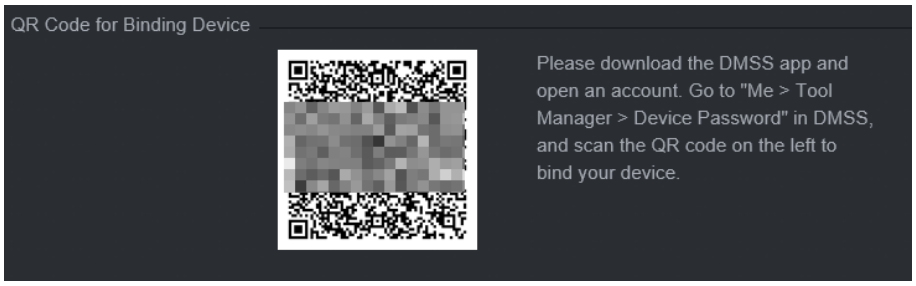
This function is enabled by default.

Step 3 Enter an email address to receive the security code used to reset the password.

Step 4 Configure security questions and answers.

Step 5 (Optional) Follow the on-screen instructions to bind the Device to DMSS app.

Figure 5-266 Bind device



Step 6 Click **OK**.

5.13.3.2 Resetting Password on Local Page

Procedure

Step 1 Right-click the live page and then select any item on the shortcut menu.

- If you have configured unlock pattern, the unlock pattern login window is displayed. Click **Forgot Pattern** to switch to password login.
- If you did not configure unlock pattern, the password login window is displayed.

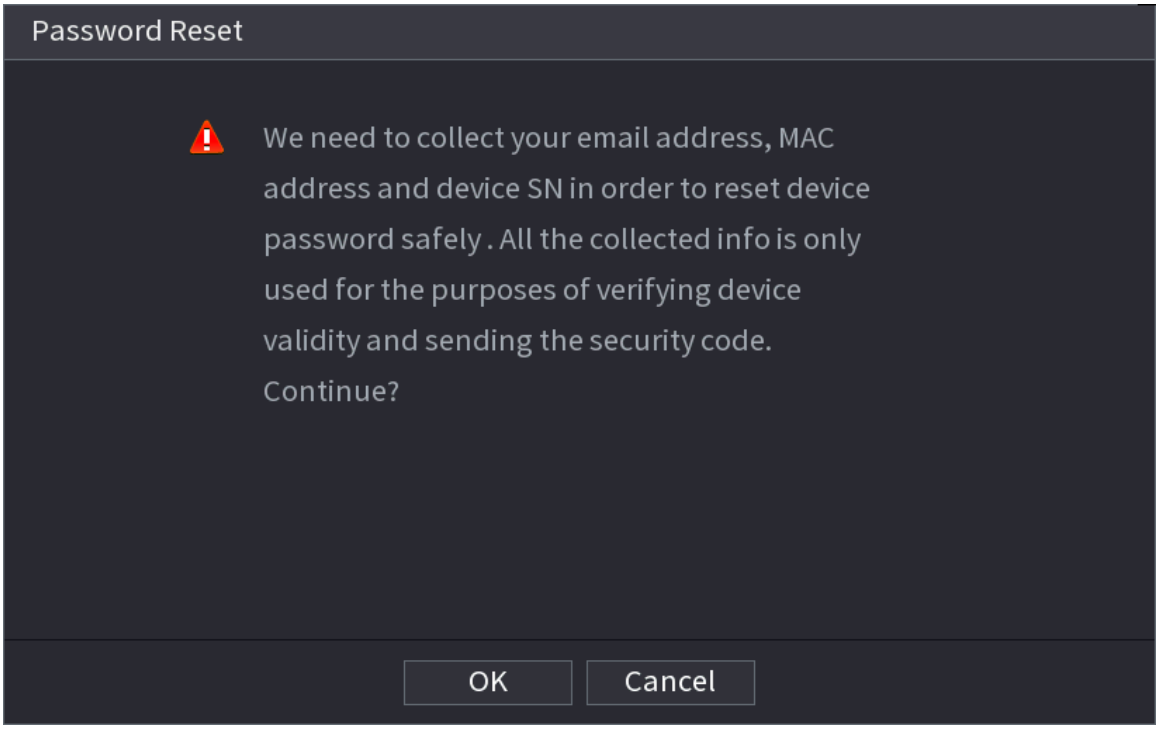
Figure 5-267 Pattern login

Figure 5-268 Password login

Step 2 Click .

- If you have set the linked email address, the system will notify you of data collection required for resetting password. Click **OK**.
- If you did not set the linked email address, the system prompts you to enter an email address. Enter the email address and then click **Next**. Then the system will notify you of data collection required for resetting password.

Figure 5-269 Notification on data collection



Step 3 Read the prompt and then click **OK**.

Step 4 Click **Next**.

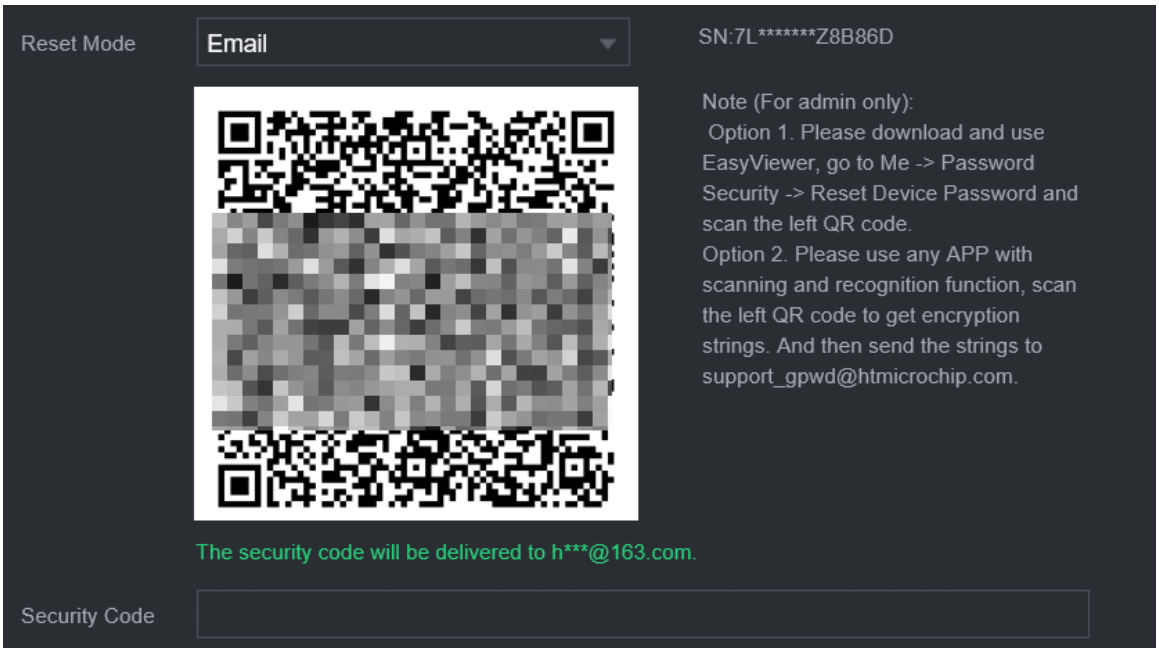
After clicking **Next** , the system will collect your information for password reset, purpose and the information includes but not limited to email address, MAC address, and device serial number. Read the prompt carefully before clicking **Next**.

Step 5 Reset the password.

- Email.

  Select **Email** as the reset mode, and then follow the on-screen instructions to get the security code in your linked email address. After that, enter the security code in the **Security Code** box.

Figure 5-270 Reset mode (email)



- App.

  Select **QR Code for Binding Device** as the reset mode, and then follow the on-screen instructions to get the security code on the DMSS app. After that, enter the security code in the **Security Code** box.

Figure 5-271 Reset mode (app)

- Security question.

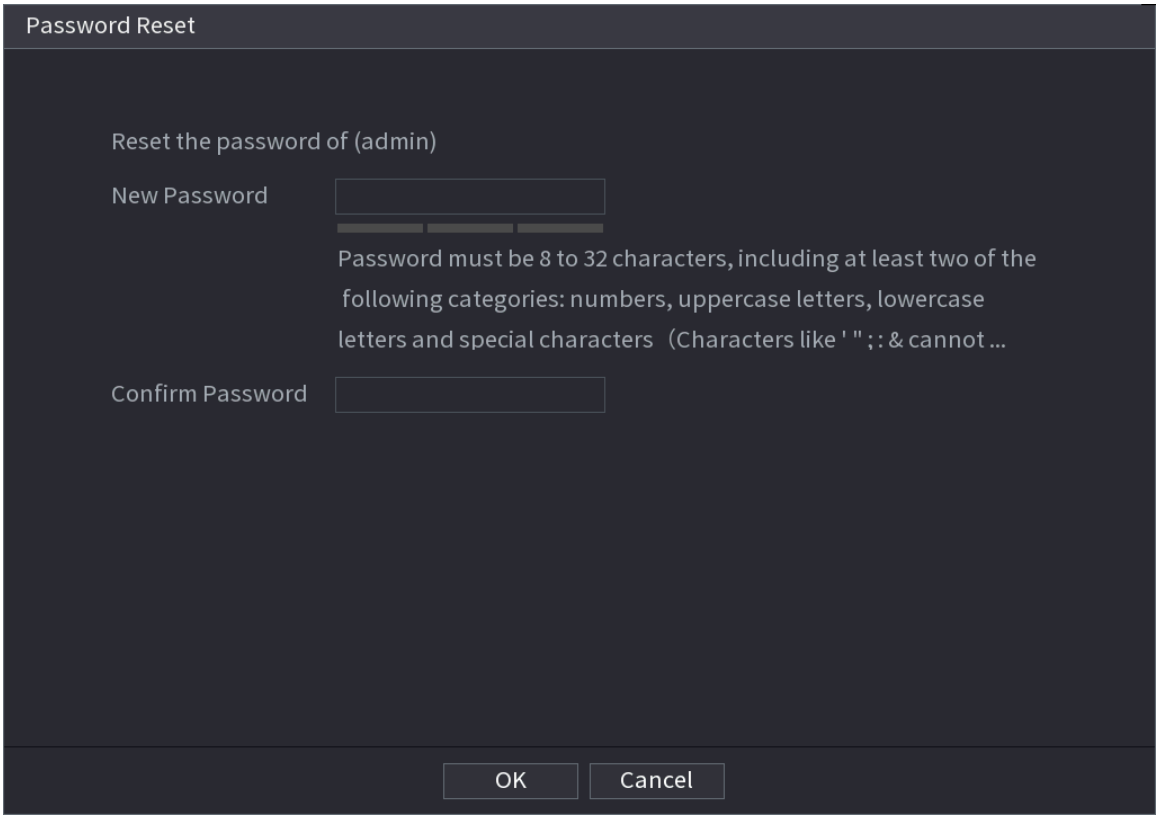
  Select **Security Question** as reset mode and then answer the security questions.

  If you did not configure the security questions in advance , **Security Question** is not available on the **Reset Mode** list.

Step 6 Click **Next**.

Step 7 Enter the new password and then enter the password again to confirm it.

Figure 5-272 Enter new password



Step 8 Click **OK**.

The password is reset.

Step 9 (Optional) When the system prompts whether to synchronize the password with the remote devices accessed through the private protocol, click **OK** to synchronize the password.

5.13.4 ONVIF User

Background Information

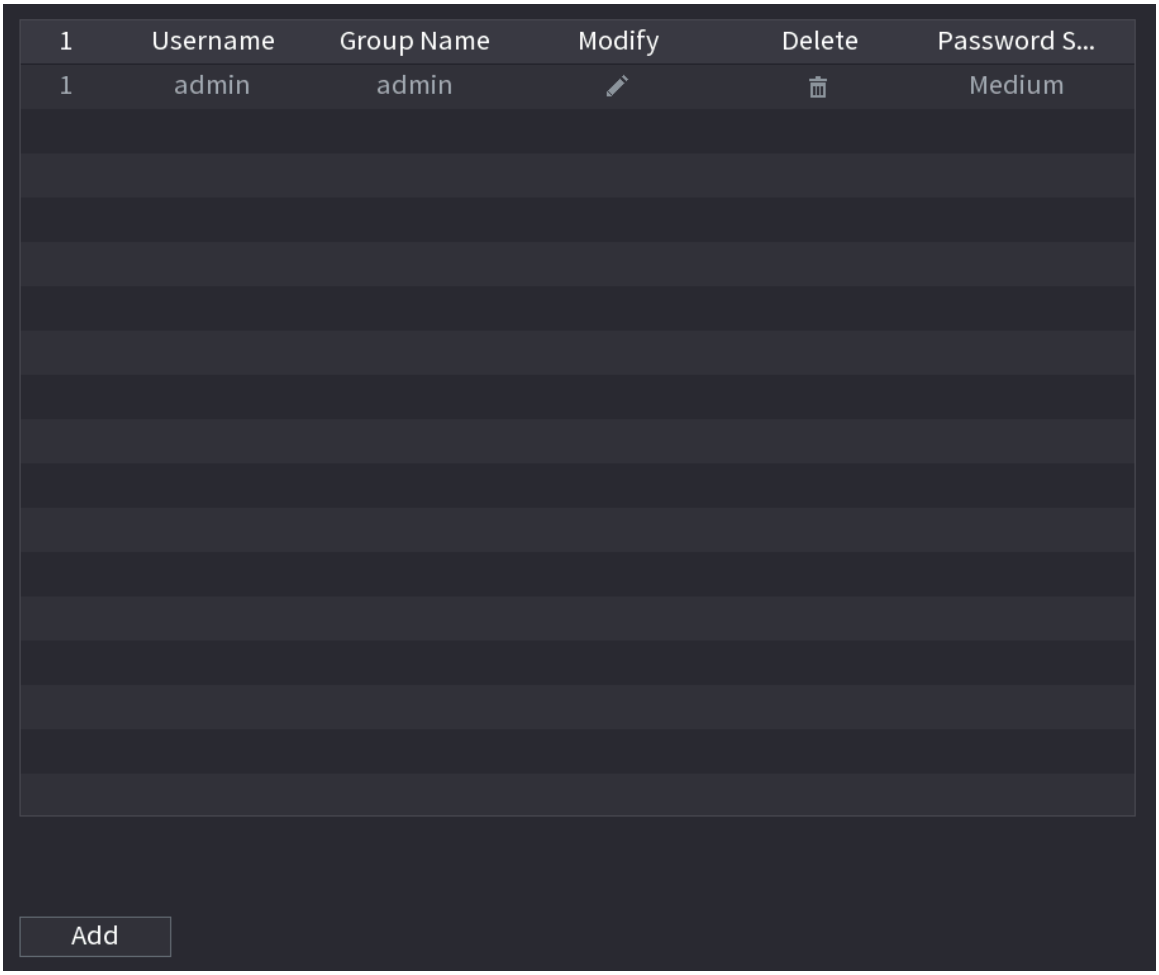
To connect the camera from the third party to the NVR via the ONVIF protocol, you need to use a verified ONVIF account.

The default ONVIF user is **admin**. It is created after you initialize the NVR and cannot be deleted.

Procedure

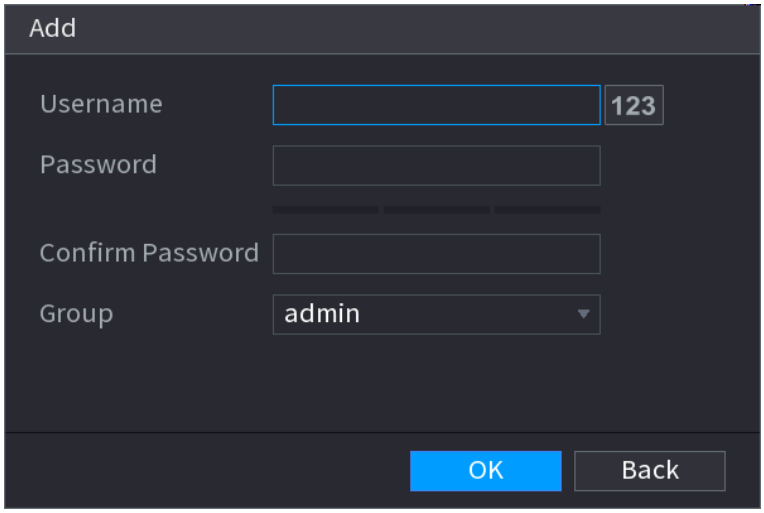
Step 1 Select **Main Menu** > **ACCOUNT** > **ONVIF User**.

Figure 5-273 ONVIF user



Step 2 Click **Add**.

Figure 5-274 Add ONVIF user



Step 3 Configure username, password and user group.

Step 4 Click **OK**.

Click to modify the corresponding user information, click to delete current user.

5.14 Security

5.14.1 Security Status

Security scanning helps get a whole picture of device security status. You can scan user, service and security module status for detailed information on the security status of the device.

Detecting User and Service

Green icon represents a healthy status of the scanned item, and orange icon represents a risky status.

- Login authentication: When there's a risk in the device configuration, the icon will be in orange to warn risk. You can click **Details** to see the detailed risk description.
- User Status: When one of device users or ONVIF users uses weak password, the icon will be in orange to warn risk. You can click **Details** to optimize or ignore the risk warning.

Figure 5-275 Security status

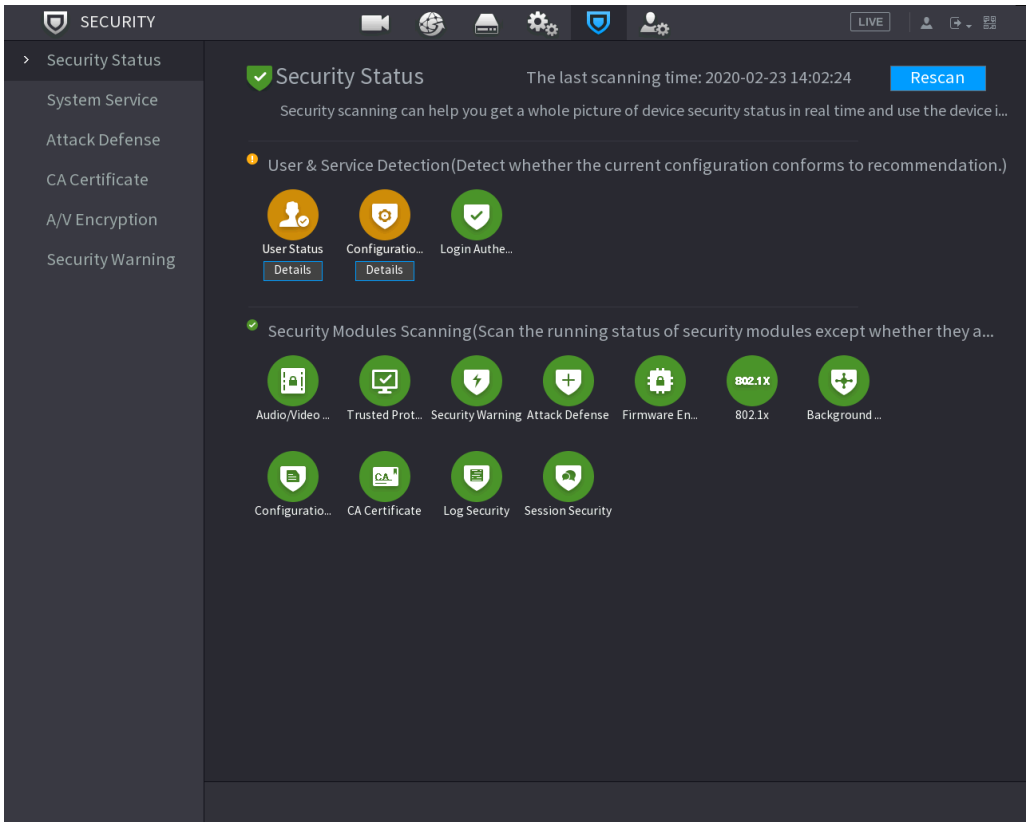
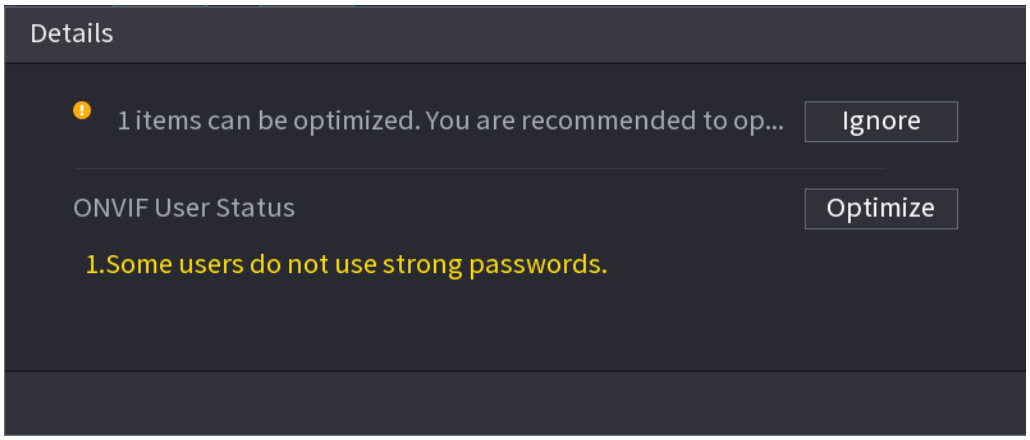
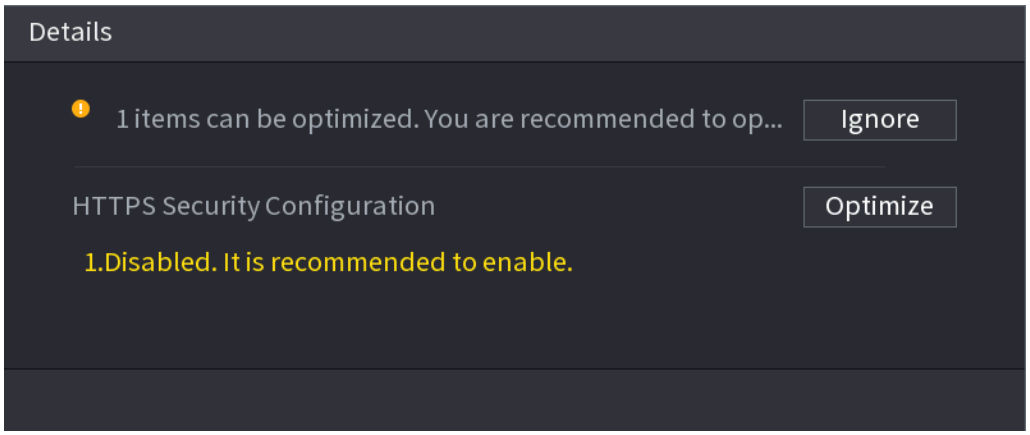


Figure 5-276 Details (1)



- Configuration Security: When there's a risk in the device configuration, the icon will be in orange to warn risk. You can click **Details** to see the detailed risk description.

Figure 5-277 Details (2)



Scanning Security Modules

This area shows the running status of security modules. For details about the security modules, point to the icon to see the on-screen instructions.

Re-scanning Security Status

You can click **Rescan** to scan security status.

5.14.2 System Service

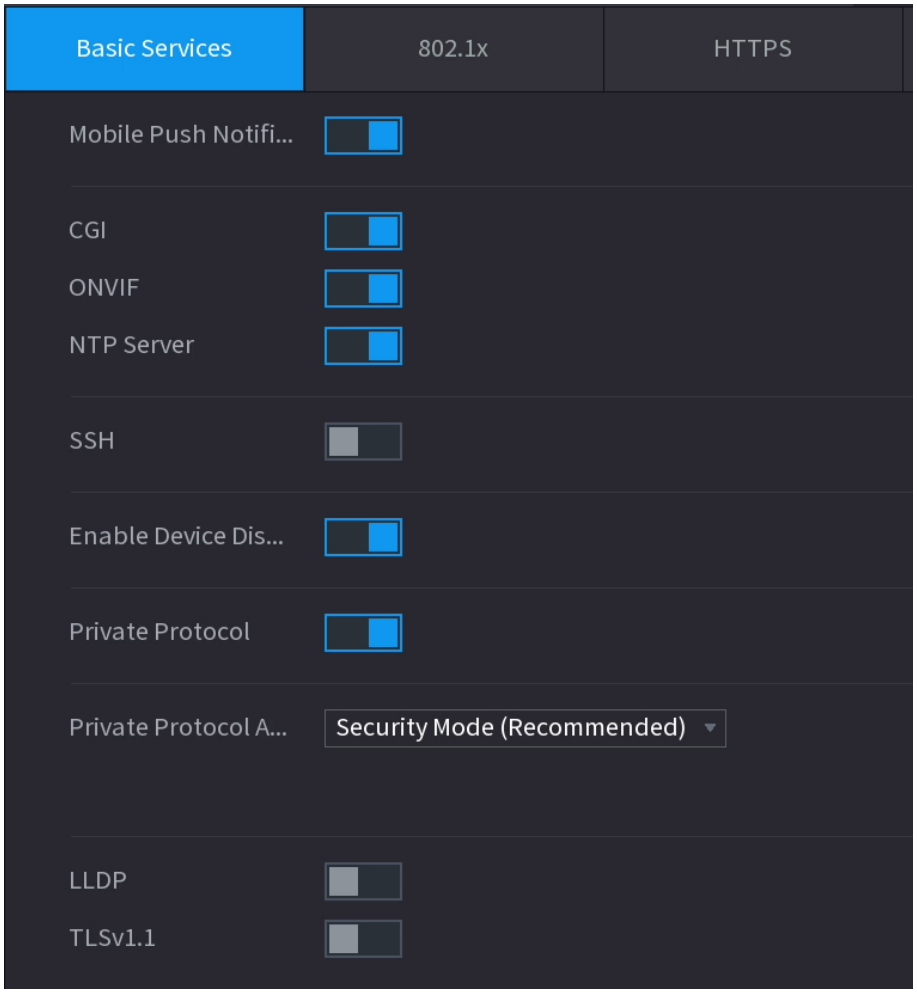
You can set NVR basic information such as basic services, 802.1x and HTTPS.

5.14.2.1 Basic Services

Procedure

Step 1 Select **Main Menu** > **SECURITY** > **System Service** > **Basic Services**.

Figure 5-278 Basic services



Step 2 Enable the system services.

There might be safety risk when **Mobile Push Notifications**, **CGI**, **ONVIF**, **SSH** and **NTP Server** is enabled. Disable these functions when they are not needed.

Table 5-78 Basic service parameters

Parameter	Description
Mobile Push Notifications	After enabling this function, the alarm triggered by the NVR can be pushed to a mobile phone. This function is enabled by default.
CGI	If this function is enabled, the remote devices can be added through the CGI protocol. This function is enabled by default.
ONVIF	If this function is enabled, the remote devices can be added through the ONVIF protocol. This function is enabled by default.
NTP Server	After enabling this function, a NTP server can be used for time synchronization. This function is enabled by default.
SSH	After enabling this function, you can use SSH service. This function is disabled by default.

Parameter	Description
Enable Device Discovery	After enabling this function, the NVR can be found by other devices through searching.
Private Protocol Authentication Mode	• Security Mode (Recommended): Uses Digest access authentication when connecting to NVR. • Compatible Mode: Select this mode when the client does not support Digest access authentication.
LLDP	Enable the LLDP service. The Link Layer Discovery Protocol (LLDP) allows two different devices to collect hardware and protocol information about neighboring devices, which is useful in troubleshooting the network.
TLSv1.1	Enable the TLSv1.1 encryption protocol.

Step 3 Click **Apply**.

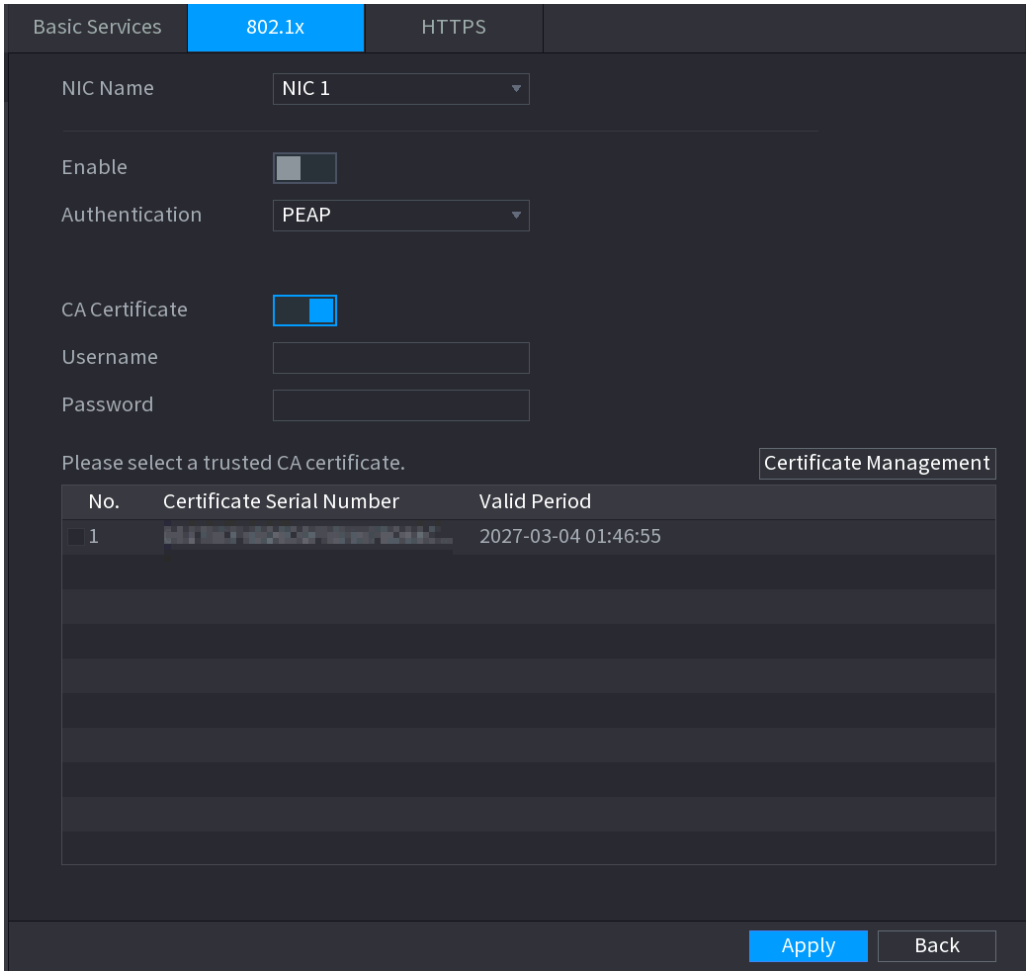
5.14.2.2 802.1x

The Device needs to pass 802.1x certification to enter the LAN.

Procedure

Step 1 Select **Main Menu** > **SECURITY** > **System Service** > **802.1x**.

Figure 5-279 802.1x



Step 2 Select the Ethernet card you want to certify.

Step 3 Select **Enable** and configure parameters.

Table 5-79 802.1x parameters

Parameter	Description
Authentication	• PEAP: protected EAP protocol. • TLS: Transport Layer Security. Provide privacy and data integrity between two communications application programs.
CA Certificate	Enable it and click **Browse** to import CA certificate from flash drive. For details about importing and creating a certificate, see "5.14.4 CA Certificate".
Username	The username shall be authorized at server.
Password	Password of the corresponding username.

Step 4 Click **Apply**.

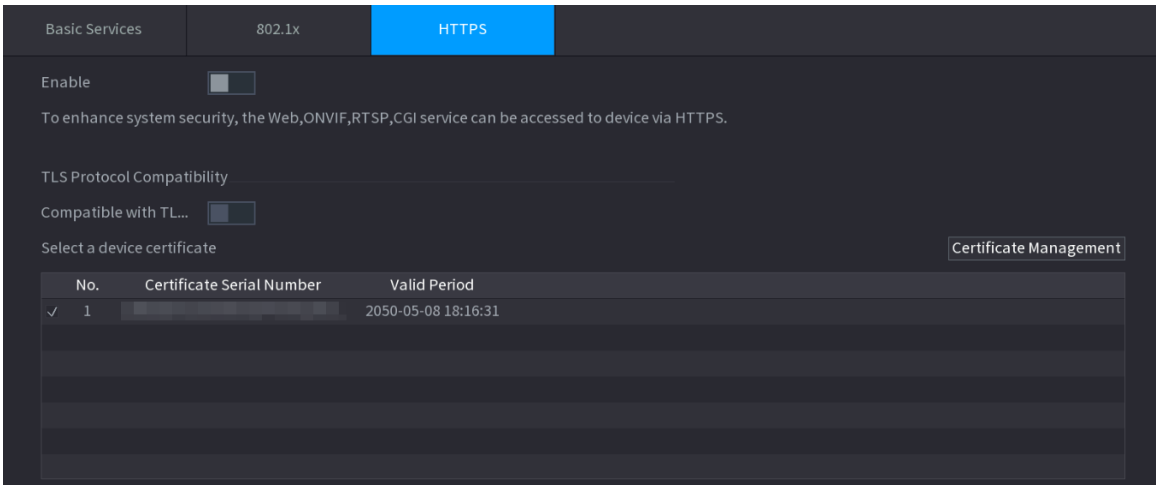
5.14.2.3 HTTPS

We recommend you enable HTTPS function to enhance system security.

Procedure

Step 1 Select **Main Menu** > **SECURITY** > **System Service** > **HTTPS**.

Figure 5-280 HTTPS



Step 2 Enable HTTPS function.

Step 3 (Optional) Enable **Compatible with TLSv1.1 and earlier versions** to allow protocol compatibility.

Step 4 Click **Certificate Management** to create or import a HTTPS certificate from USB drive. For details about importing or creating a CA certificate, see "5.14.4 CA Certificate".

Step 5 Select a HTTPS certificate.

Step 6 Click **Apply**.

5.14.3 Attack Defense

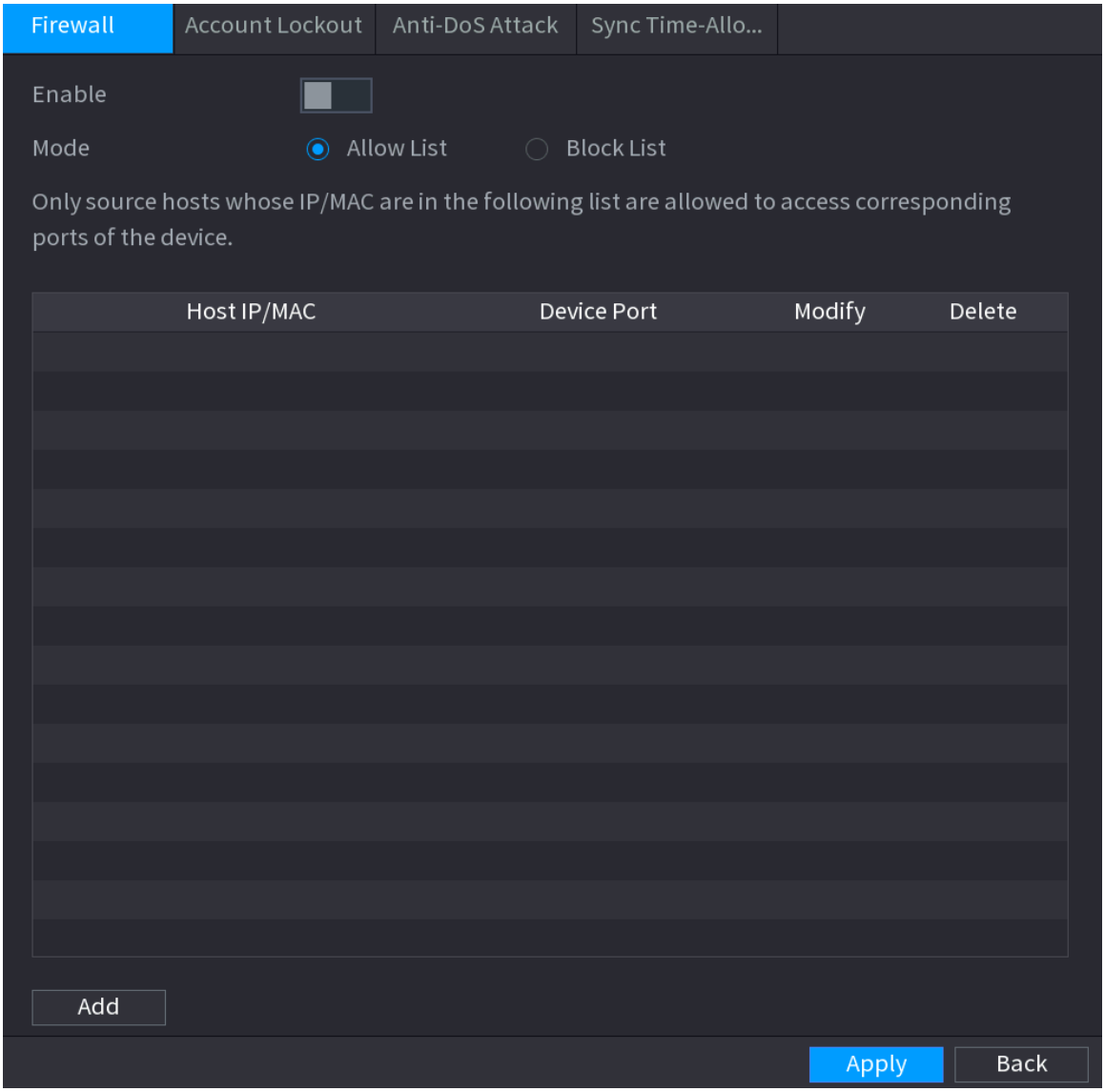
5.14.3.1 Firewall

You can configure the hosts that are allowed or prohibited to access the Device.

Procedure

Step 1 Select **Main Menu** > **SECURITY** > **Attack Defense** > **Firewall**.

Figure 5-281 Firewall



Step 2 Click to enable the firewall.

Step 3 Select a firewall mode.

- **Allow List** : The hosts on the allowlist can access the Device.
- **Block List** : The hosts on the blocklist are prohibited to access the Device.

Step 4 Click **Add** and then select a type for the allowlist or blocklist.

You can allow or prohibit hosts through a specific IP address, a network segment, or a MAC address.

- IP address.

  Enter the IP address, start port and end port, and then click **OK**.
- IP segment.

  Enter the start address and end address, starting port and ending port, and then click **OK**.
- MAC address.

  Enter the MAC address, and then click **OK**.

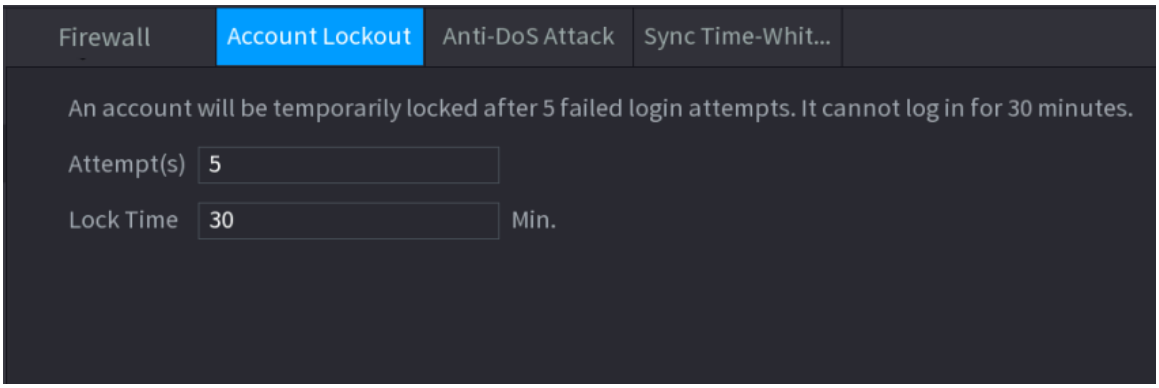
Step 5 Click **Apply**.

5.14.3.2 Account Lockout

Procedure

Step 1 Select **Main Menu** > **SECURITY** > **Attack Defense** > **Account Lockout**.

Figure 5-282 Account lockout



Step 2 Set parameters.

Table 5-80 Account lockout parameters

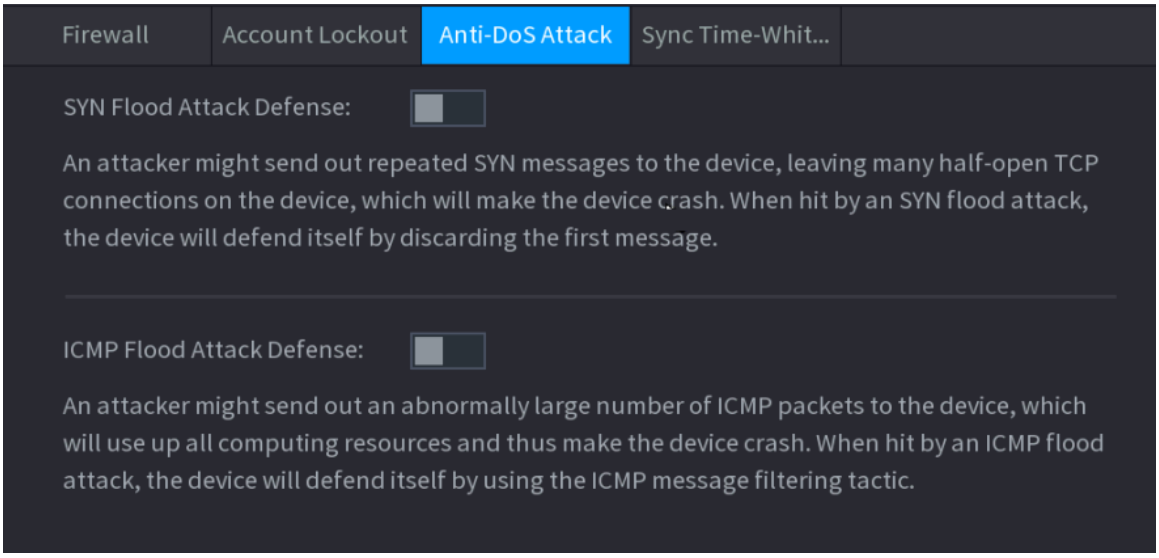
Parameter	Description
Attempt(s)	Set the maximum number of allowable wrong password entries. The account will be locked after your entries exceed the maximum number.
Lock Time	Set how long the account is locked for.

Step 3 Click **Apply**.

5.14.3.3 Anti-DoS Attack

You can enable **SYN Flood Attack Defense** and **ICMP Flood Attack Defense** to defend the Device against Dos attack.

Figure 5-283 Anti-Dos Attack



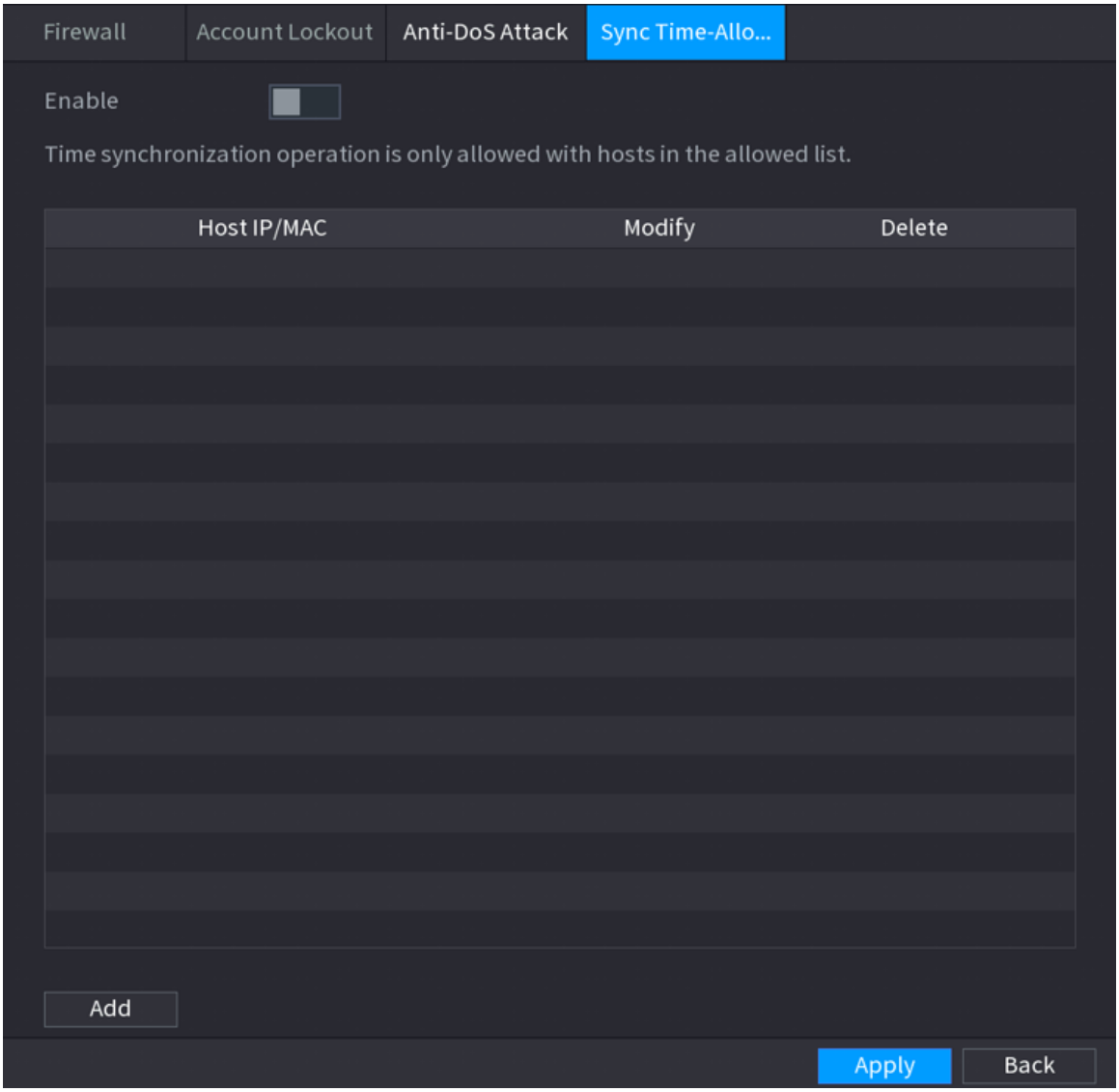
5.14.3.4 Sync Time-Allowlist

You can configure which hosts are allowed to synchronize time with the Device.

Procedure

Step 1 Select **Main Menu** > **SECURITY** > **Attack Defense** > **Sync Time-Allowlist**.

Figure 5-284 Sync Time-Allowlist



Step 2 Click to enable the function.

Step 3 Click **Add** to add trusted hosts for time synchronization.

- If you set **Type** to **IP Address**, enter the IP address, and then click **OK**.
- If you set **Type** to **IP Segment**, enter the start address and end address, and then click **OK**.

Step 4 Click **Apply**.

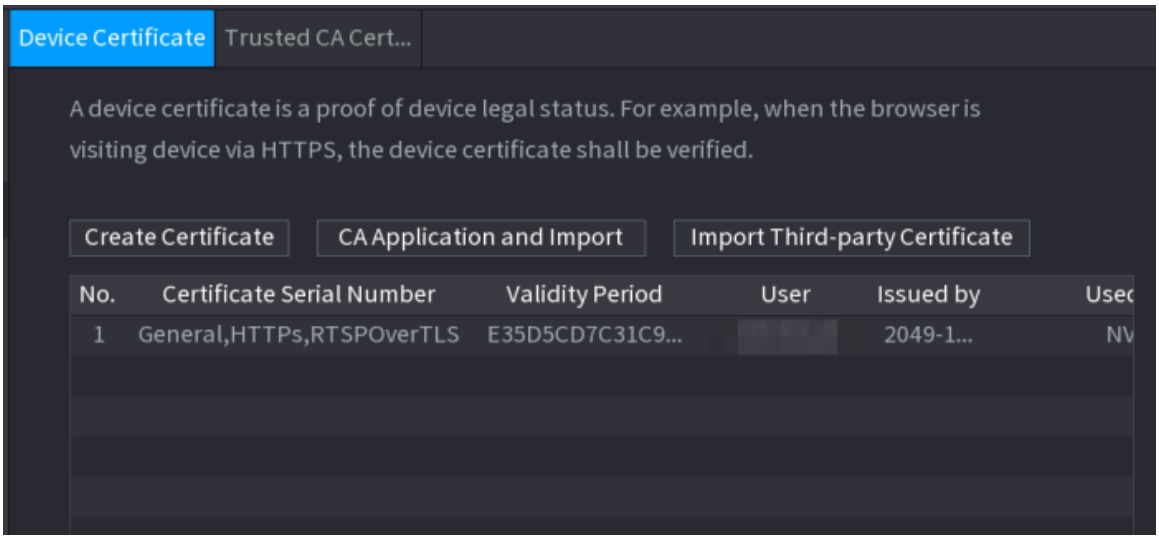
5.14.4 CA Certificate

5.14.4.1 Device Certificate

Create Certificate

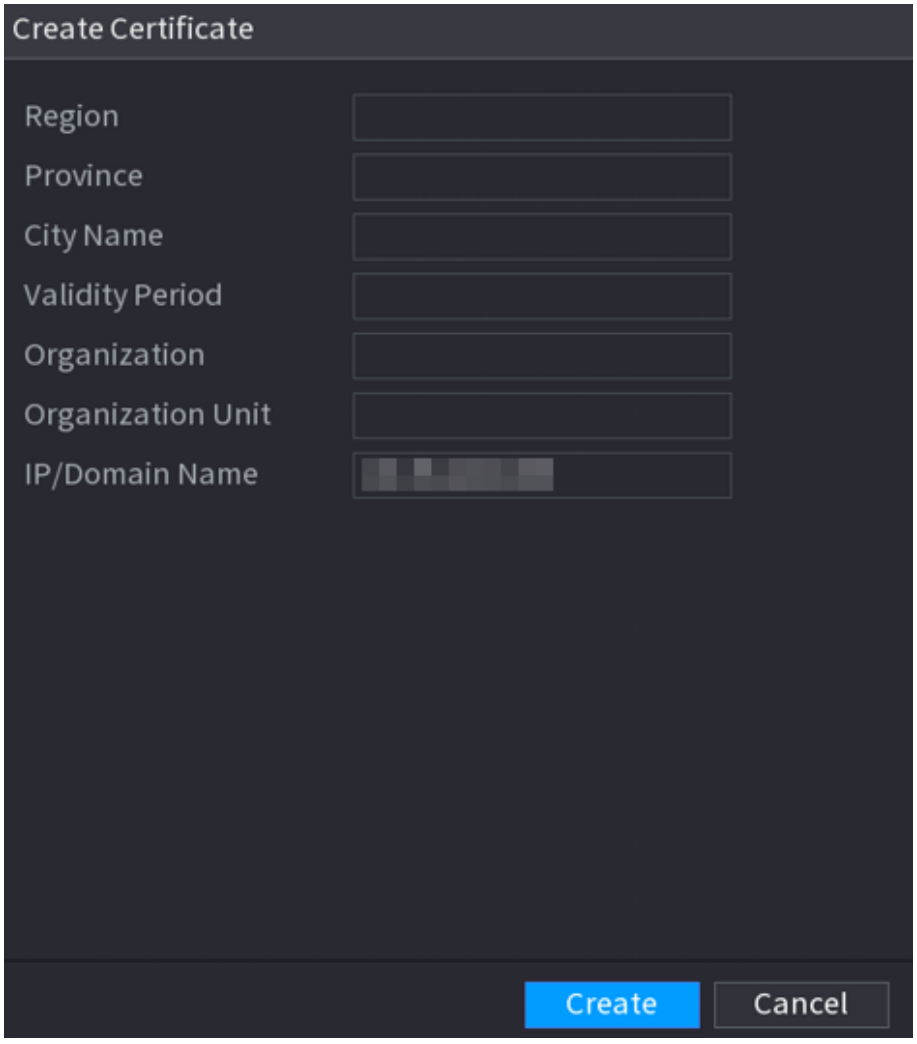
1. Select **Main Menu** > **SECURITY** > **CA Certificate** > **Device Certificate**.

Figure 5-285 Device certificate



2. Click **Create Certificate**.

Figure 5-286 Create certificate

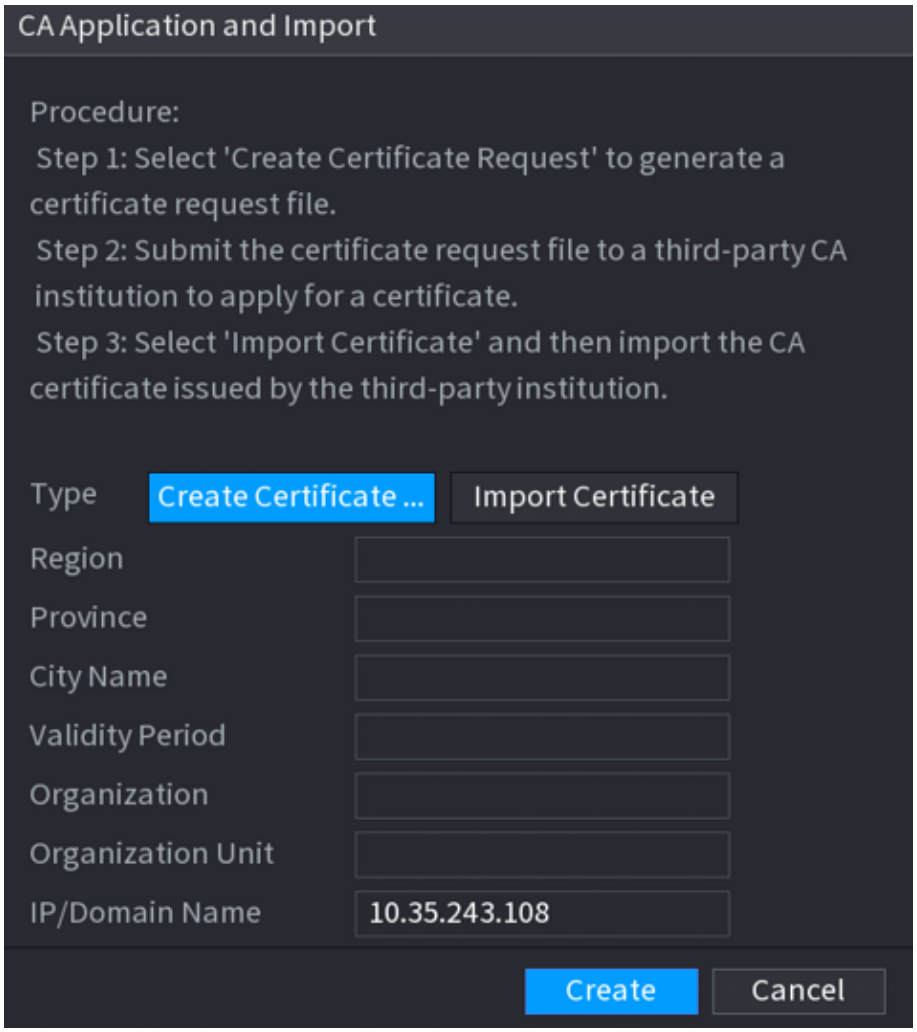


3. Configure the parameters.
4. Click **Create**.

CA Application and Import

Click **CA Application and Import** and then follow the on-screen instructions to finish CA application and import.

Figure 5-287 CA application and import



Import Third-Party Certificate

1. Click **Import Third-Party Certificate**
2. Configure the parameters.

Table 5-81 Parameters for importing third-party certificate

Parameter	Description
Path	Click **Browse** to find the third-party certificate path on the USB drive.
Private Key	Click **Browse** to find the third-party certificate private key on the USB drive.
Private Key Password	Input the private key password.

3. Click **Create**.

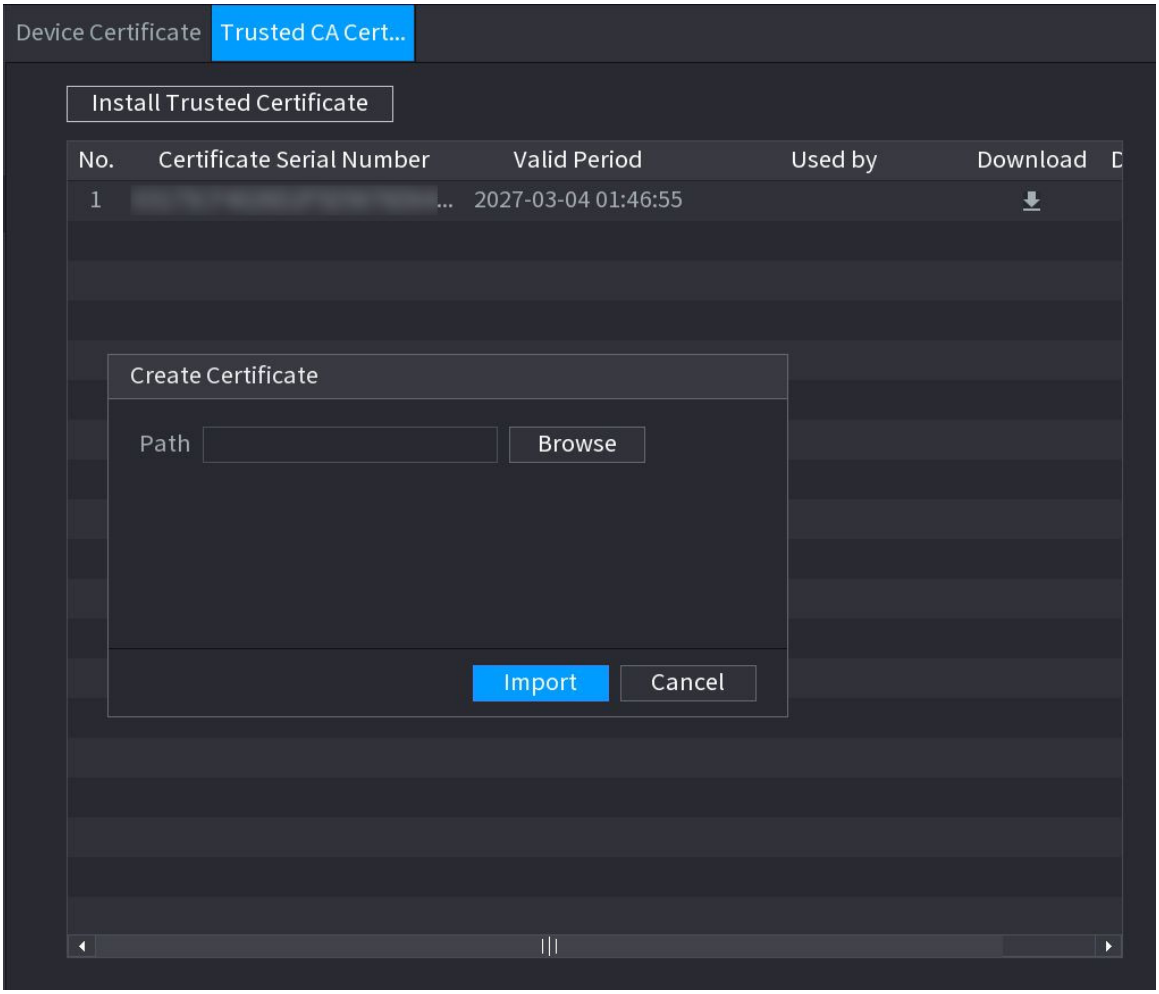
5.14.4.2 Trusted CA Certificate

Procedure

Step 1 Select **Main Menu** > **SECURITY** > **CA Certificate** > **Trusted CA Certificate**.

Step 2 Click **Install Trusted Certificate**.

Figure 5-288 Create certificate



Step 3 Click **Browse** to select the certificate that you want to install.

Step 4 Click **Import**.

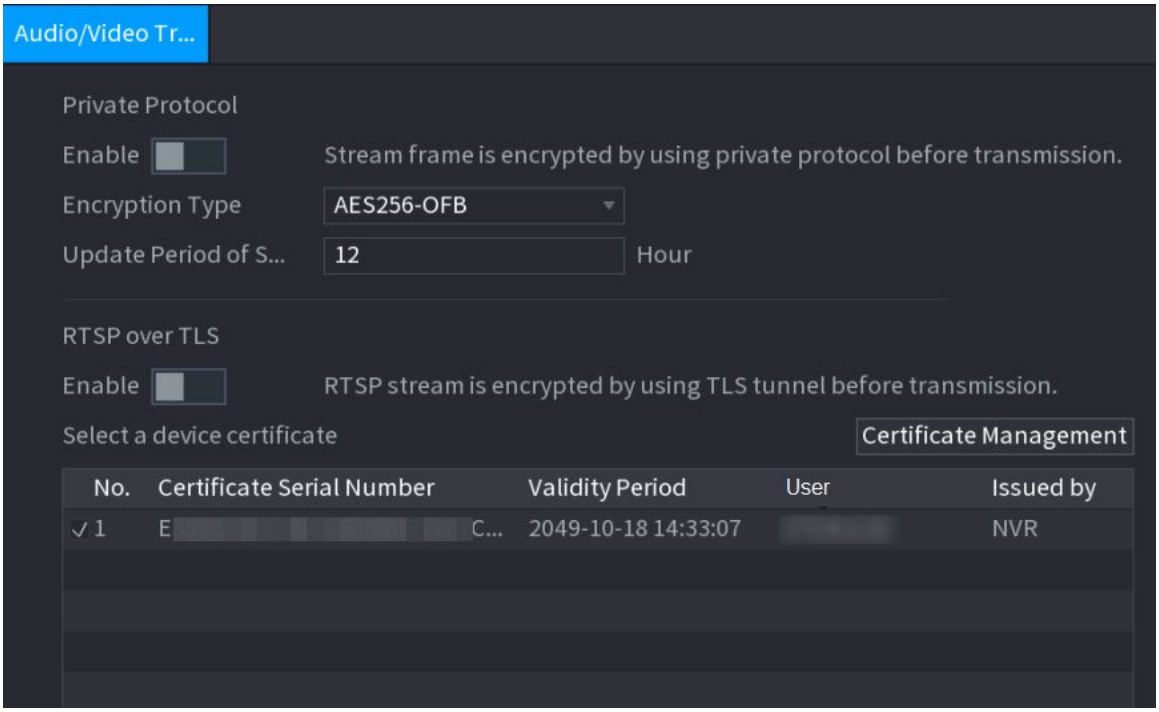
5.14.5 Audio/Video Encryption

The Device supports audio and video encryption during data transmission.

Procedure

Step 1 Select **Main Menu** > **SECURITY** > **AUDIO/VIDEO ENCRYPTION** > **Audio/Video Transmission**.

Figure 5-289 Audio and video transmission



Step 2 Configure parameters.

Table 5-82 Audio and video transmission parameters

Area	Parameter	Description
Private Protocol	Enable	Enables stream frame encryption by using private protocol. There might be safety risk if this service is disabled.
	Encryption Type	Use the default setting.
	Update Period of Secret Key	Secret key update period. Value range: 0–720 hours. 0 means never update the secret key. Default value: 12.
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS. There might be safety risk if this service is disabled.
	Select a device certificate	Select a device certificate for RTSP over TLS.
	Certificate Management	For details about certificate management, see "5.14.4.1 Device Certificate".

Step 3 Click **Apply**.

5.14.6 Security Warning

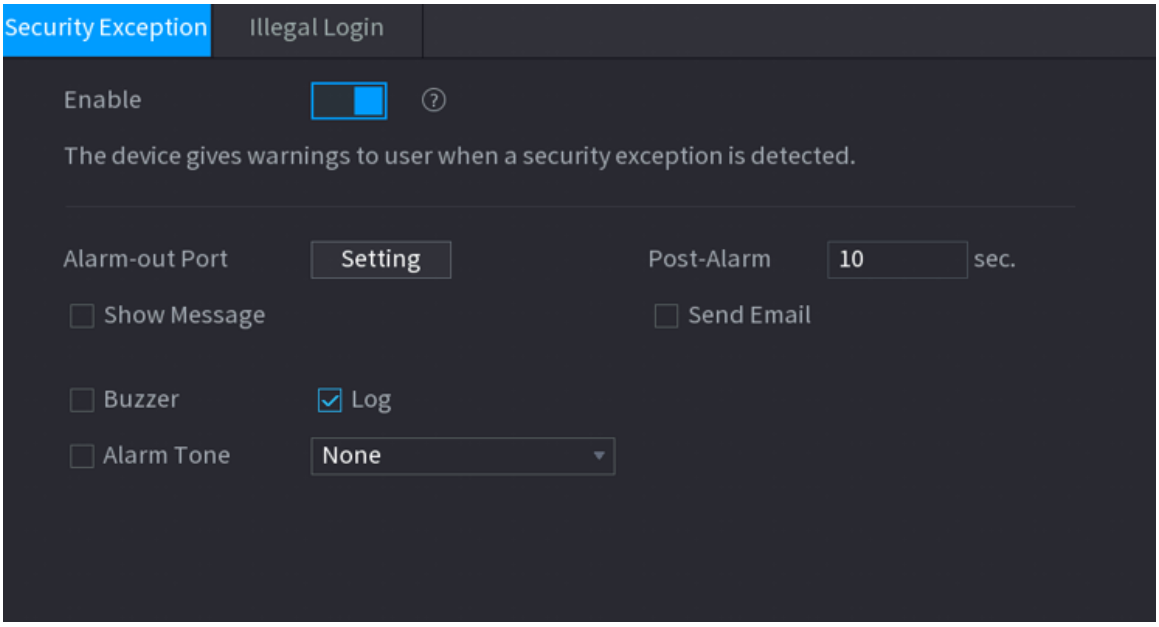
5.14.6.1 Security Exception

The Device gives warnings to the user when a security exception occurs.

Procedure

Step 1 Select **Main Menu** > **SECURITY** > **Security Warning** > **Security Exception**.

Figure 5-290 Security exception



Step 2 Click to enable the function.

Click to view the list of security exception events.

Step 3 Configure alarm linkage actions. For details, see Table 5-50 .

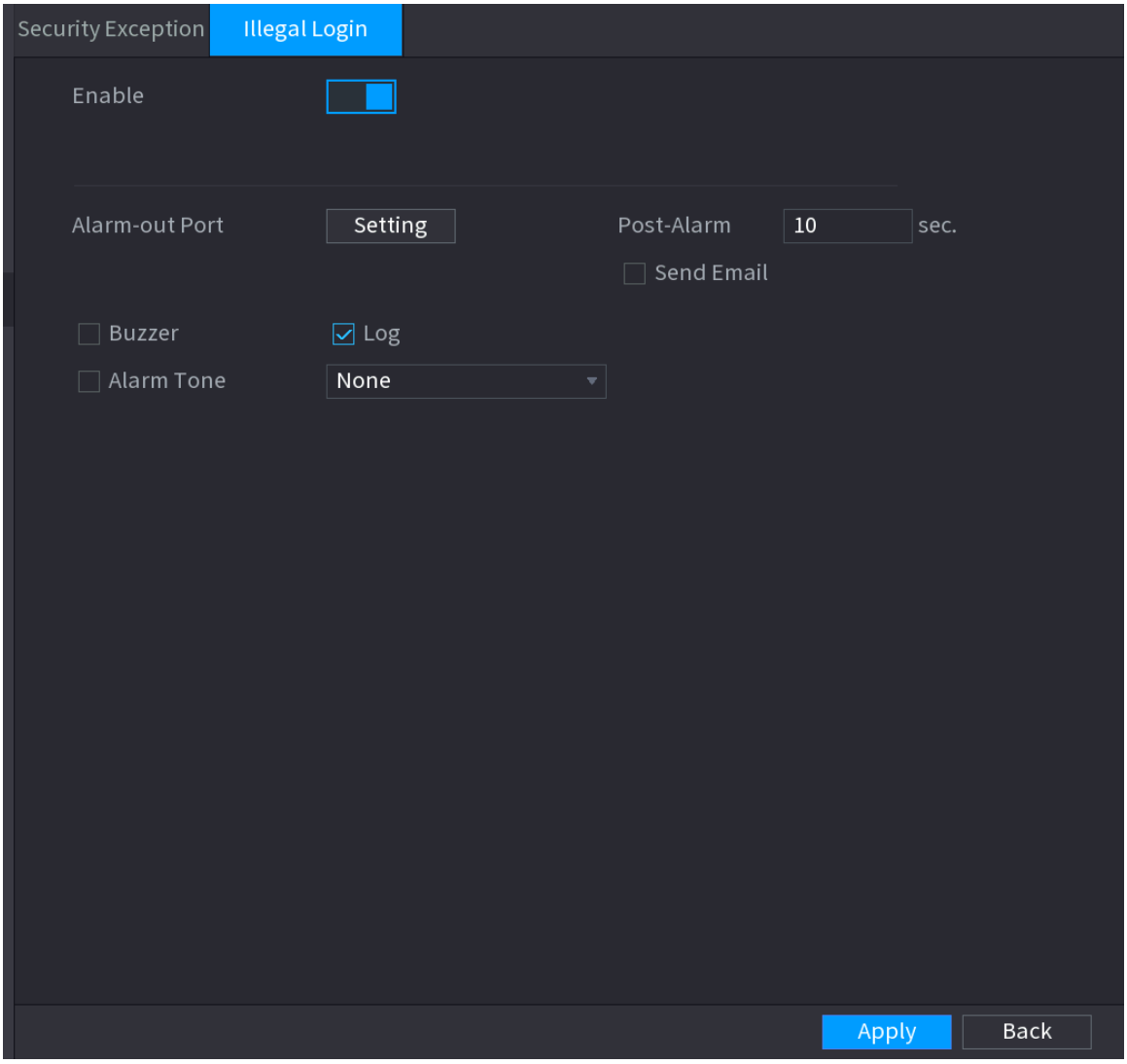
Step 4 Click **Apply**.

5.14.6.2 Illegal Login

Procedure

Step 1 Select **Main Menu** > **SECURITY** > **Security Warning** > **Illegal Login**.

Figure 5-291 Illegal login



Step 2 Click to enable the function.

Step 3 Configure alarm linkage actions. For details, see Table 5-50 .

Step 4 Click **Apply**.

5.15 System

5.15.1 General Settings

You can set NVR basic information such as system date and holiday.

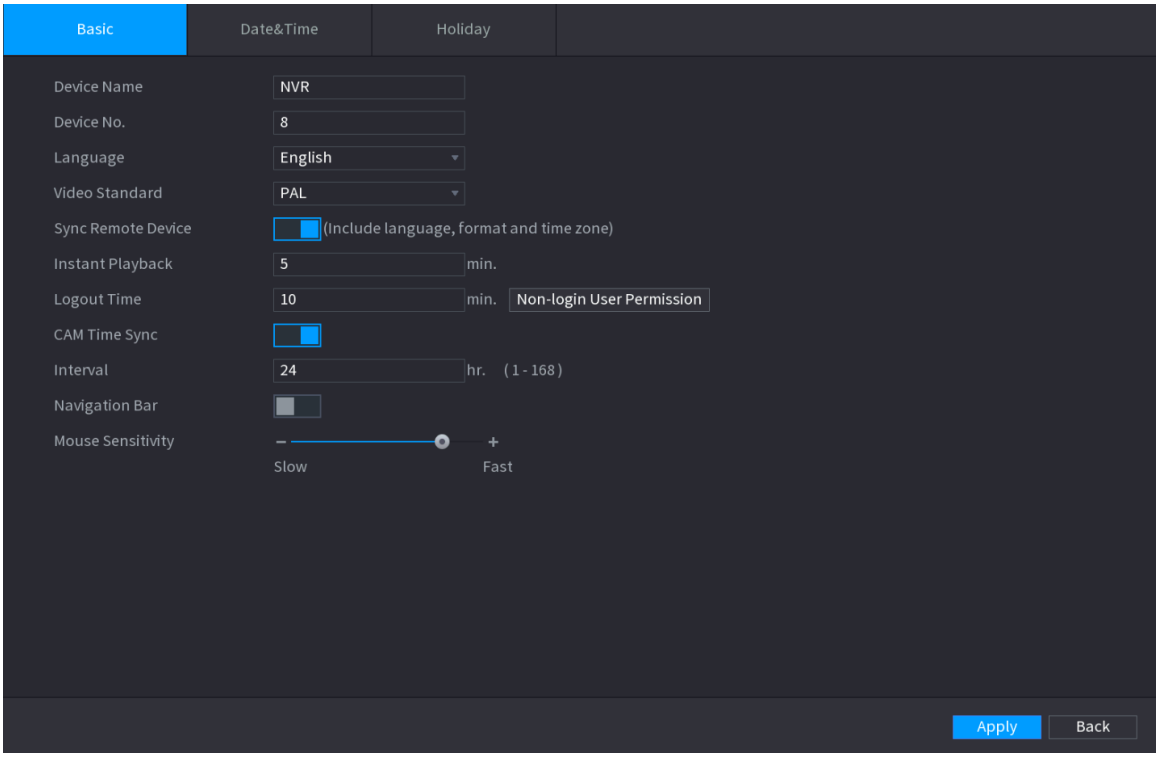
5.15.1.1 General

You can set device basic information such as device name, and serial number.

Procedure

Step 1 Select **Main Menu** > **SYSTEM** > **General** > **Basic**.

Figure 5-292 Basic settings



Step 2 Set parameters.

Table 5-83 Basic parameters

Parameter	Description
Device Name	Enter the Device name.
Device No.	Enter a number for the Device.
Language	Select a language for the Device system.
Video Standard	Select **PAL** or **NTSC** as needed.
Sync Remote Device	Enable this function; the NVR can synchronize information with the remote device such as Language, video standard and time zone.
Instant Playback	In the **Instant Play** box, enter the time length for playing back the recorded video. The value ranges from 5 to 60. On the live view control bar, click the instant playback button to play back the recorded video within the configured time.
Logout Time	Enter the standby time for the Device. The Device automatically logs out when it is not working in the configured period. You need to login the Device again. The value ranges from 0 to 60. 0 indicates there is not standby time for the Device. Click **Monitor Channel(s) when logout**. You can select the channels that you want to continue monitoring when you logged out.
CAM Time Sync	Syncs the Device time with IP camera.

Parameter	Description
Interval	Enter the interval for time sync.
Logout Time	You can set auto logout interval once login user remains inactive for a specified time. Value ranges from 0 to 60 minutes.
Navigation Bar	Enable the navigation bar. When you click on the live view screen, the navigation bar is displayed.
Mouse Sensitivity	Adjust the speed of double-click by moving the slider. The bigger the value is, the faster the speed is.

Step 3 Click **Apply** button to save settings.

5.15.1.2 Date and Time

Background Information

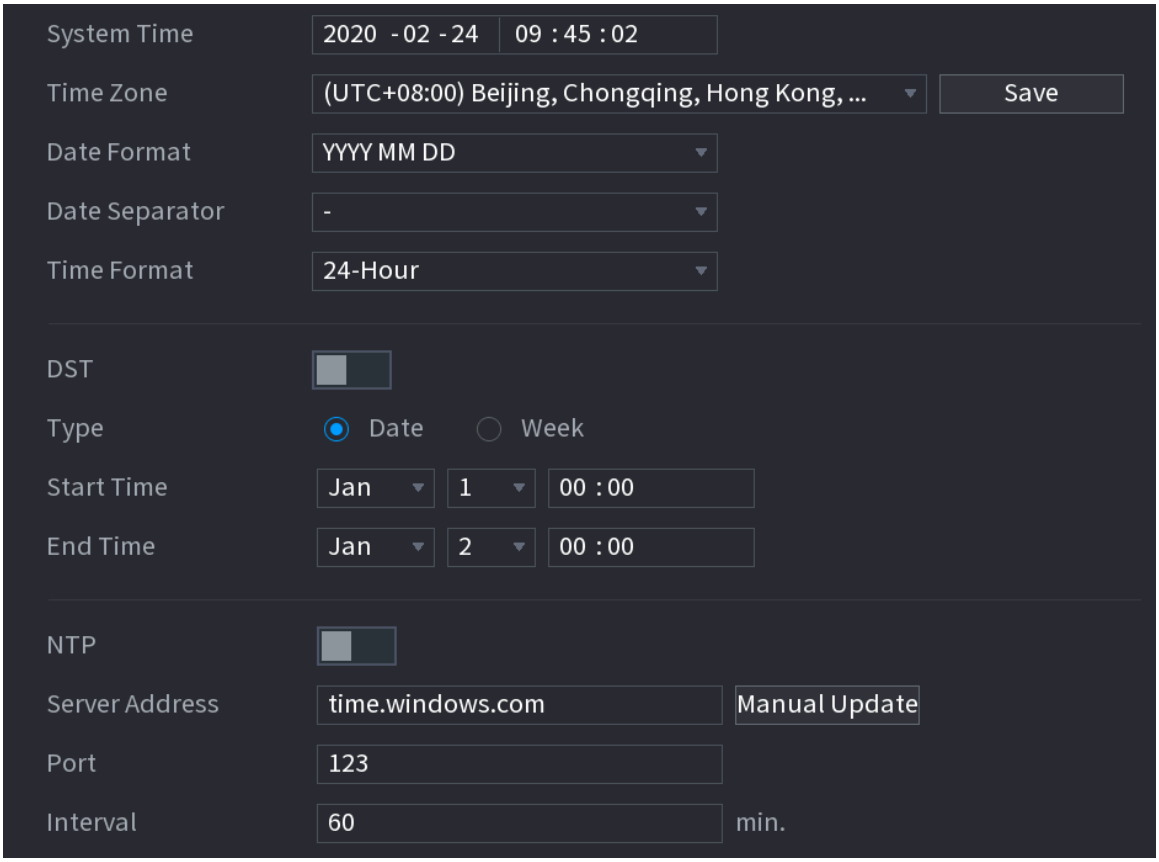
You can set device time. You can enable NTP (Network Time Protocol) function so that the device can sync time with the NTP server.

You can also configure date and time settings by selecting **Main Menu** > **SYSTEM** > **General** > **Date&Time**.

Procedure

Step 1 Click **Date&Time** tab.

Figure 5-293 Date and time



Step 2 Configure the settings for date and time parameters.

Table 5-84 Data and time parameters

Parameter	Description
System Time	In the **System Time** box, enter time for the system. Click the time zone list, you can select a time zone for the system, and the time in adjust automatically. Do not change the system time randomly; otherwise the recorded video cannot be searched. It is recommended to avoid the recording period or stop recording first before you change the system time.
Time Zone	In the **Time Zone** list, select a time zone for the system.
Date Format	In the **Date Format** list, select a date format for the system.
Date Separator	In the **Date Separator** list, select a separator style for the date.
Time Format	In the **Time Format** list, select **12-HOUR** or **24-HOUR** for the time display style.
DST	Enable the Daylight Saving Time function. Click **Week** or **Date**.
Start Time	Configure the start time and end time for the DST.
End Time	
NTP	Enable the NTP function to sync the Device time with the NTP server. If NTP is enabled, device time will be automatically synchronized with server.
Server Address	In the **Server Address** box, enter the IP address or domain name of the corresponding NTP server. You can directly select **time.windows.com** or **time.google.com**. Click **Manual Update**, the Device starts syncing with the server immediately.
Port	The system supports TCP protocol only and the default setting is 123.
Interval	In the **Interval** box, enter the amount of time that you want the Device to sync time with the NTP server. The value ranges from 0 to 65535.

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

5.15.1.3 Holiday

Background Information

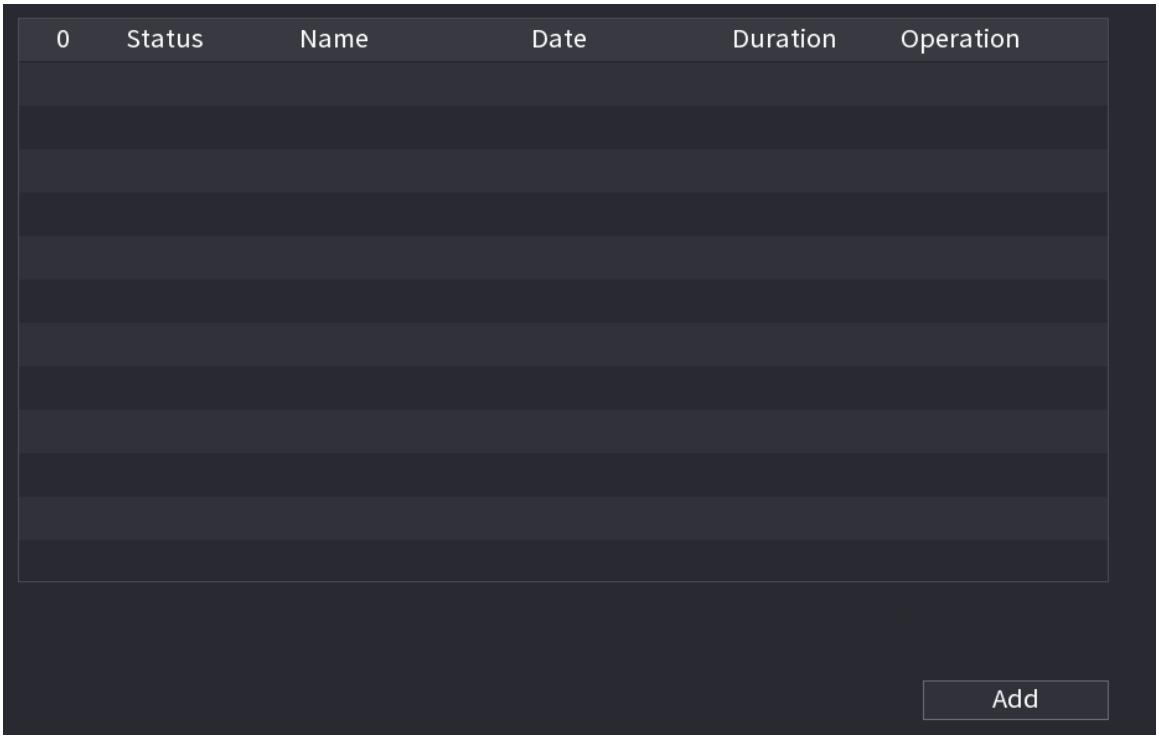
Here you can add, edit, and delete holiday. After you successfully set holiday information, you can view holiday item on the record and snapshot period.

You can also configure holiday settings by selecting **Main Menu** > **SYSTEM** > **General** > **Holiday**.

Procedure

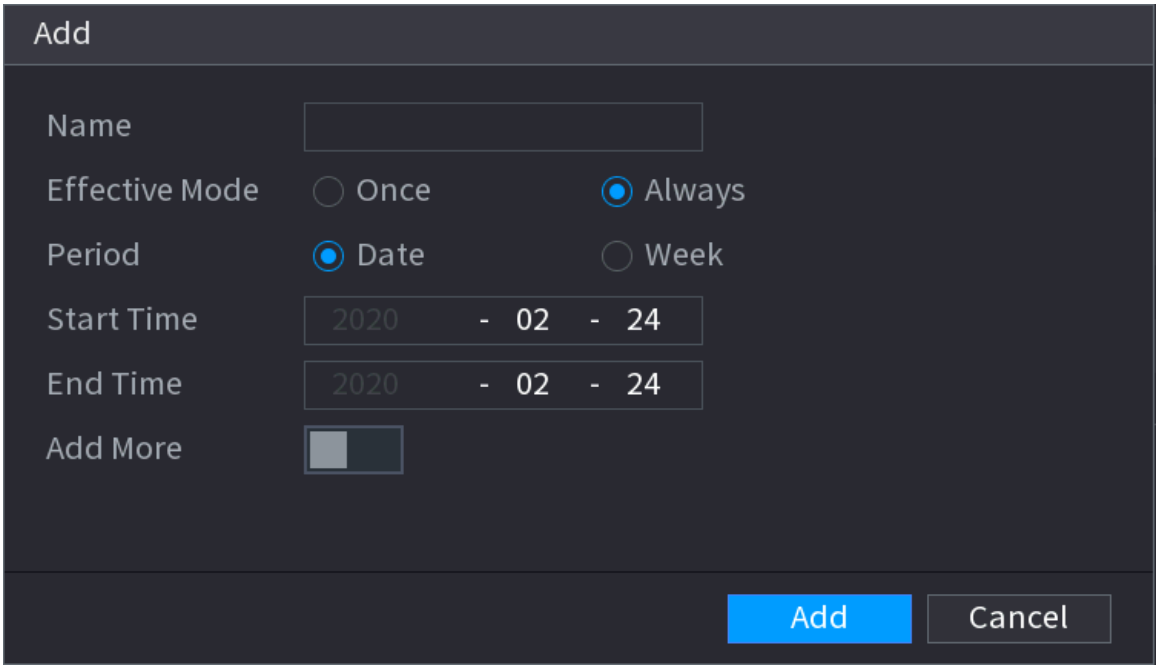
Step 1 Click **Next**.

Figure 5-294 Holiday



Step 2 Click **Add Holidays**.

Figure 5-295 Add holidays



Step 3 Set holiday name, repeat mode and holiday mode.

Click **Add more** to add new holiday information.

Step 4 Click **Add**, you can add current holiday to the list.

- Click the drop-down list of the state; you can enable/disable holiday date.
- Click to change the holiday information. Click to delete current date.

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

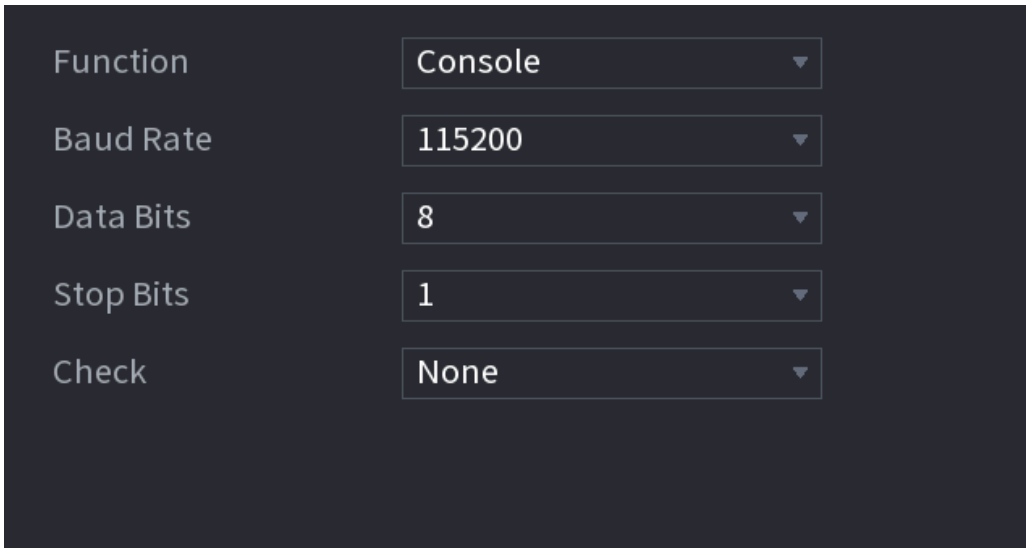
5.15.2 Serial Port

After setting RS-232 parameters, the NVR can use the COM port to connect to other device to debug and operate.

Procedure

Step 1 Select **MAIN MENU** > **SYSTEM** > **Serial Port**.

Figure 5-296 Serial port



Step 2 Configure parameters.

Table 5-85 Serial port parameters

Parameter	Description
Function	Select serial port control protocol. • Console: Upgrade the program and debug with the console and mini terminal software. • Keyboard: Control this Device with special keyboard. • Adapter: Connect with PC directly for transparent transmission of data. • Protocol COM: Configure the function to protocol COM, in order to overlay card number. • PTZ Matrix: Connect matrix control Different series products support different RS-232 functions.
Baud Rate	Select baud rate, which is 115200 by default.

Parameter	Description
Data Bits	It ranges from 5 to 8, which is 8 by default.
Stop Bits	It includes 1 and 2.
Parity	It includes none, odd, even, mark and null.

Step 3 Click **Apply**.

5.16 Output and Display

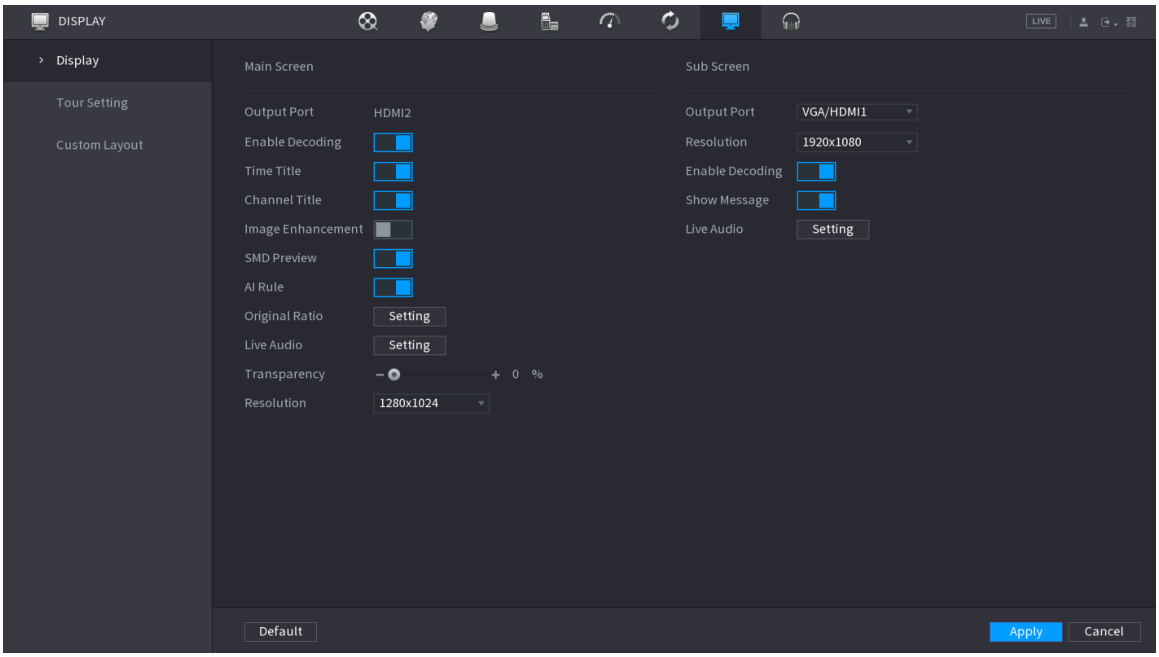
5.16.1 Display

You can configure the display effect such as displaying time title and channel title, adjusting image transparency, and selecting the resolution.

Procedure

Step 1 Select **Main Menu** > **DISPLAY** > **Display**.

Figure 5-297 Display



Step 2 Configure the parameters.

Table 5-86 Display parameters

Parameter	Description
Main Screen/Sub Screen	Configure the output port format of both screens. ● When sub screen is disabled, the format of main screen is HDMI/VGA simultaneous output. ● When sub screen is enabled, the format of main screen and sub screen are non-simultaneous outputs. ◇ When output port of sub screen is set to **HDMI** , the output port of main screen is set to **VGA** by the device. ◇ When output port of sub screen is set to **VGA** , the output port of main screen is set to **HDMI** by the device.
Enable Decoding	After it is enabled, the device can normally decode.
Time Title/Channel Title	Select the checkbox and the date and time of the system will be displayed in the preview screen.
Transparency	Set the transparency of the local menu of the NVR device. The higher the transparency, the more transparent the local menu.
Time Title/Channel Title	Select the checkbox and the date and time of the system will be displayed in the preview screen.
Image Enhancement	Select the checkbox to optimize the preview image edges.
SMD Preview	Select the checkbox to display the SMD previews in the live view page.
AI Rule	Select the checkbox to display the AI rules in the live view page. This function is for some series products only.
Original Ratio	Click **Setting** and select the channel to restore the corresponding channel image to the original scale.
Live Audio	Configure audio input on live view. You can select **Audio 1** , **Audio 2**, and **Mixing**. For example, if you select **Audio 1** for **D1** channel, the sound of audio input port 1 of camera is playing. If you select **Mixing**, the sound of all audio input ports are playing.
Resolution	Support 1920 × 1080, 1280 × 1024 (default), 1280 × 720.

Step 3 Click **Apply**.

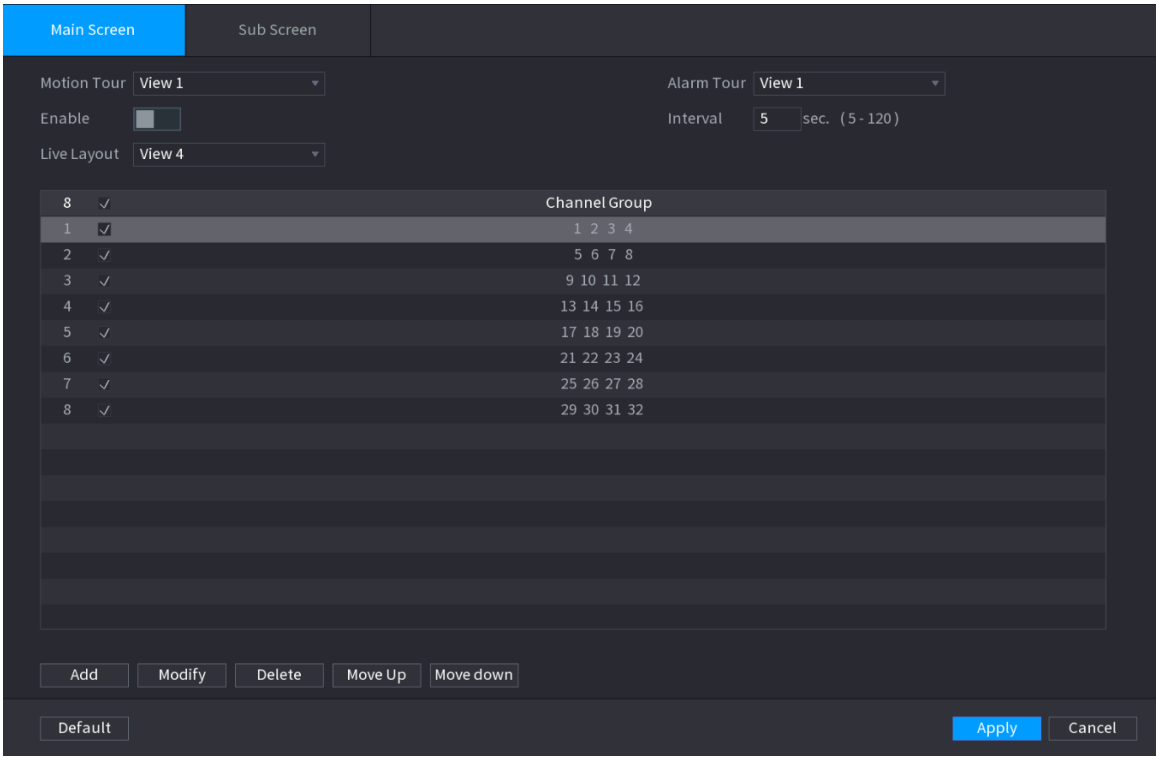
5.16.2 Tour

You can configure a tour of selected channels to repeat playing videos. The videos display in turn according to the channel group configured in tour settings. The system displays one channel group for a certain period and then automatically changes to the next channel group.

Procedure

Step 1 Select **DISPLAY** > **Tour Setting** > **Main Screen**.

Figure 5-298 Tour



- On the top right of the live view screen, use the left mouse button or press Shift to switch between (image switching is allowed) and (image switching is not allowed) to turn on/off the tour function.
- On the navigation bar, click to enable the tour and click to disable it.

Step 2 Configure the tour setting parameters.

Table 5-87 Tour parameters

Parameter	Description
Enable Tour	Enable tour function.
Interval	Enter the amount of time that you want each channel group displays on the screen. The value ranges from 5 seconds to 120 seconds, and the default value is 5 seconds.
Motion Tour, Alarm Tour	Select the View 1 or View 8 for **Motion Tour** and **Alarm Tour** (system alarm events).
Live Layout	In the **Live Layout** list, select **View 1**, **View 4**, **View 8**, or other modes that are supported by the Device.

Parameter	Description
Channel Group	Display all channel groups under the current Window Split setting. • Add a channel group: Click **Add**, in the pop-up **Add Group** channel, select the channels to form a group, and then click **Save**. • Delete a channel group: Select the checkbox of any channel group, and then click **Delete**. • Edit a channel group: Select the checkbox of any channel group and then click **Modify**, or double-click on the group. The **Modify Channel Group** dialog box is displayed. You can regroup the channels. • Click **Move up** or **Move down** to adjust the position of channel group.

Step 3 Click **Apply** to save the settings.

5.16.3 Custom Layout

Background Information

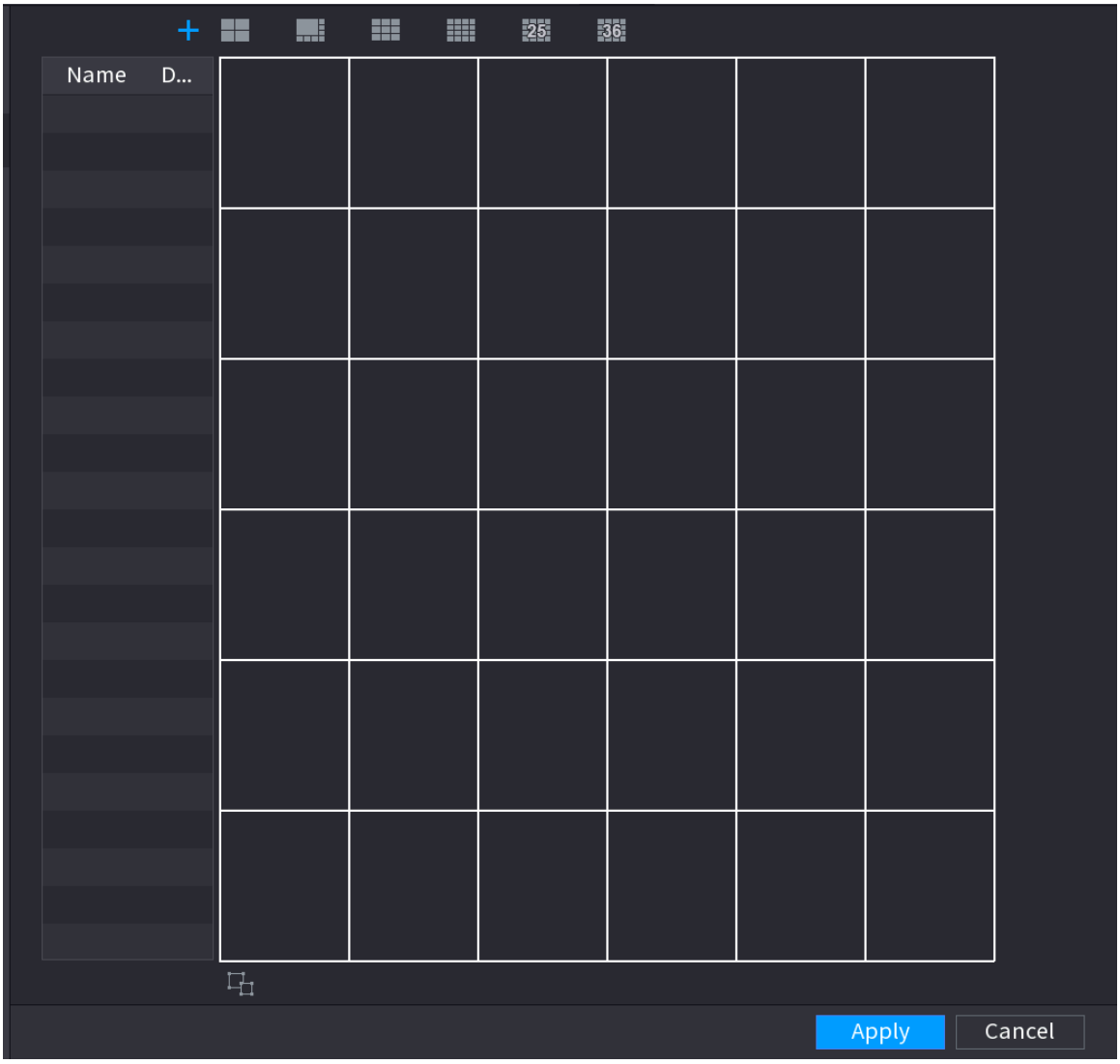
You can set customized video split mode.

- This function is for some series products. See the actual product for detailed information.
- Device max. supports 5 customized videos.

Procedure

Step 1 Select **Main Menu** > **DISPLAY** > **Custom Split**.

Figure 5-299 Custom split



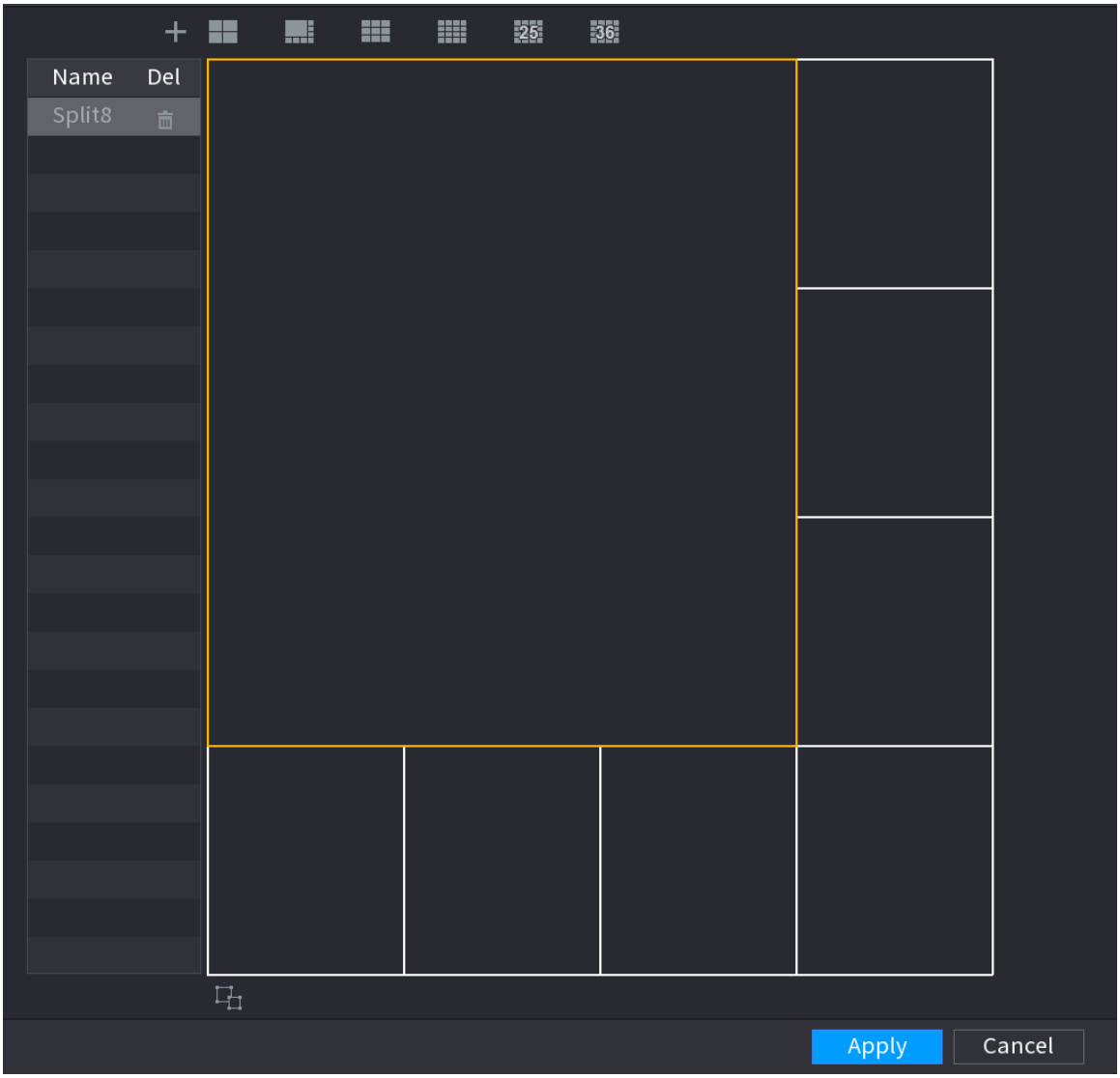
Step 2 Click and then click to select basic mode.

System adopts the basic window mode as the new window name. For example, if you select the 8 display mode, the default name is Split8.

In regular mode, drag the mouse in the preview frame; you can merge several small windows to one window so that you can get you desired split mode.

- After merge the window, system adopts the remaining window amount as the new name such as Split6.
- Select the window you want to merge (red highlighted), click to cancel the merge to restore the basic mode.
- Click to delete the customized window mode.

Figure 5-300 Merged window



Step 3 Click **Apply** to exit.

After the setup, you can go to the preview window, right-click and then select **Live Layout** to select the custom split layout.

5.17 POS

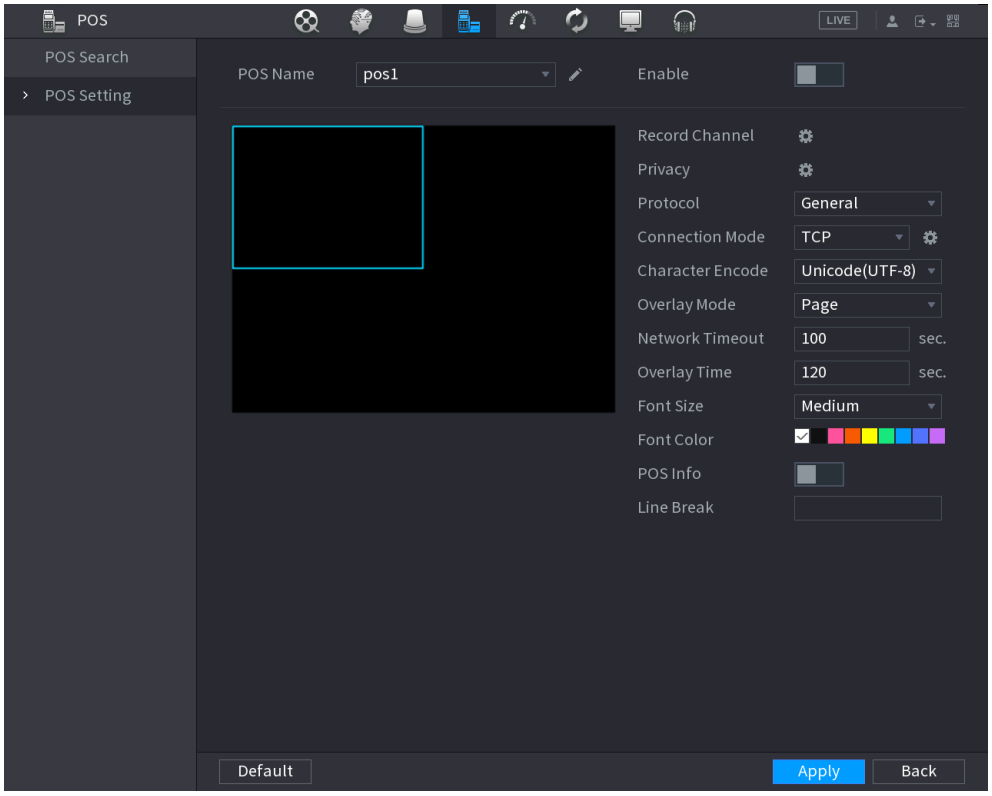
You can connect the Device to the POS (Point of Sale) machine and receive the information from it. This function applies to the scenarios such as supermarket POS machine. After connection is established, the Device can access the POS information and display the overlaid text in the channel window.

5.17.1 Settings

Procedure

Step 1 Select **Main Menu** > **POS** > **POS Setting**.

Figure 5-301 POS setting



Step 2 Configure the POS parameters.

Table 5-88 POS parameters

Parameter	Description
POS Name	In the POS Name list, select the POS machine that you want to configures settings for. Click to modify the POS name. ● The POS name must be unique. ● You can enter up to 21 Chinese characters or 63 English characters.
Enable	Enable the POS function.
Record Channel	Click to select a channel to record.
Privacy	Enter the privacy contents.
Protocol	Select a protocol. Different machines correspond to different protocols.
Connection Mode	Select the connection protocol type. Click , the **IP Address** window is displayed. In the **Source IP** box, enter the IP address (the machine that is connected to the Device) that sends messages.
Character Encode	Select a character encoding mode.

Parameter	Description
Overlay Mode	In the **Overlay Mode** list, Select **Turn** or**ROLL**. • Turn: Once the information is at 16 lines, system displays the next page. • ROLL: Once the information is at 16 lines, system rolls one line after another to delete the first line. When the local preview mode is in 4-split, the turn/ROLL function is based on 8 lines.
Network time out	When the network is not working correctly and cannot be recovered after the entered timeout limit, the POS information will not display normally. After the network is recovered, the latest POS information will be displayed.
Time Display	Enter the time that how long you want to keep the POS information displaying. For example, enter 5, the POS information disappear from the screen after 5 seconds.
Font Size	Select **Small** , **Medium**, or **Big** as the text size of POS information
Font Color	In the color bar, click to select the color for the text size of POS information.
POS Info	Enable the POS Info function, the POS information displays in the live view/ WEB.
Line Break	There is no line delimiter by default. After you set the line delimiter (HEX), the overlay information after the delimiter is displayed in the new line. For example, the line delimiter is F and the overlay information is 123F6789, NVR displays overlay information on the local preview page and Web as: 123 6789

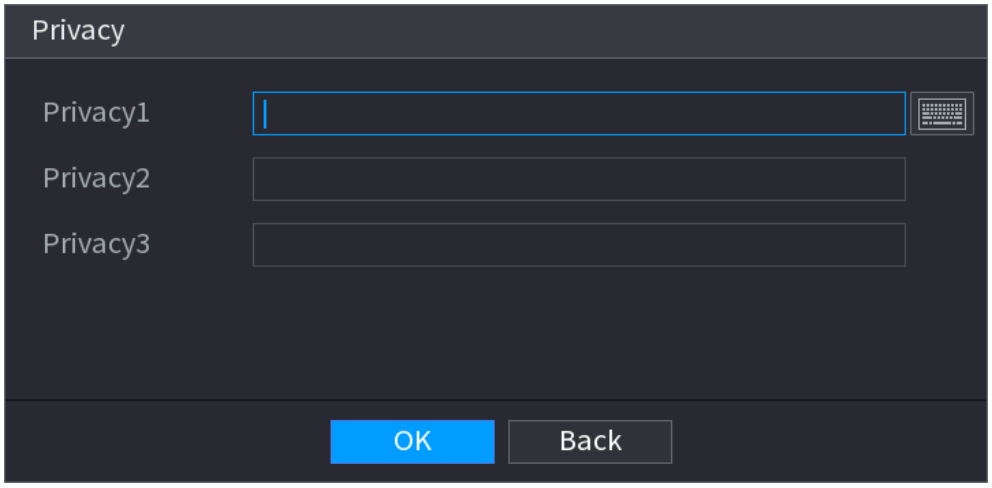
Step 3 Click **Apply**.

5.17.1.1 Privacy Setup

Procedure

Step 1 Click next to **Privacy**.

Figure 5-302 Privacy



Step 2 Set privacy information.

Step 3 Click **OK**.

5.17.1.2 Connection Mode

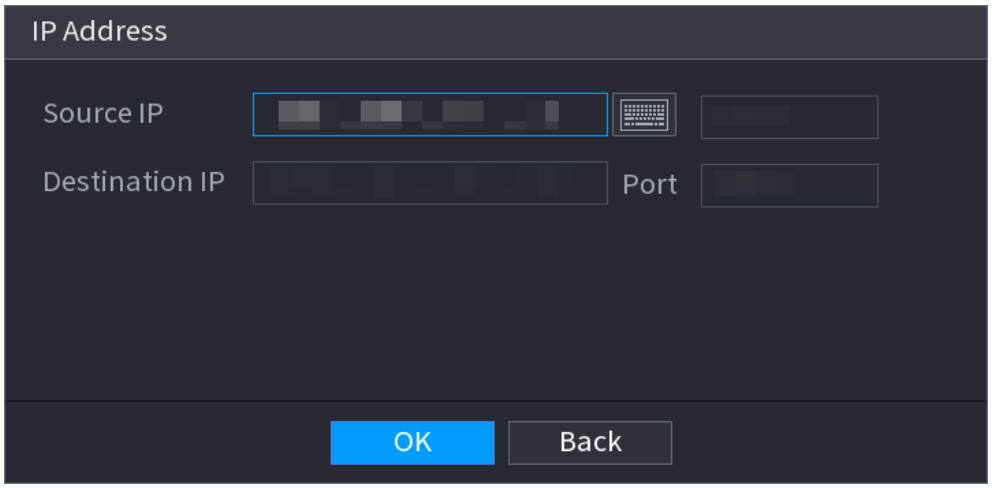
Connection type is UDP or TCP.

Procedure

Step 1 Select **Connection Mode** as **UDP**, **TCP_CLINET** or **TCP**.

Step 2 Click .

Figure 5-303 IP address



Step 3 For **Source IP** and **Port**, enter the POS IP address and port.

Step 4 Click **OK**.

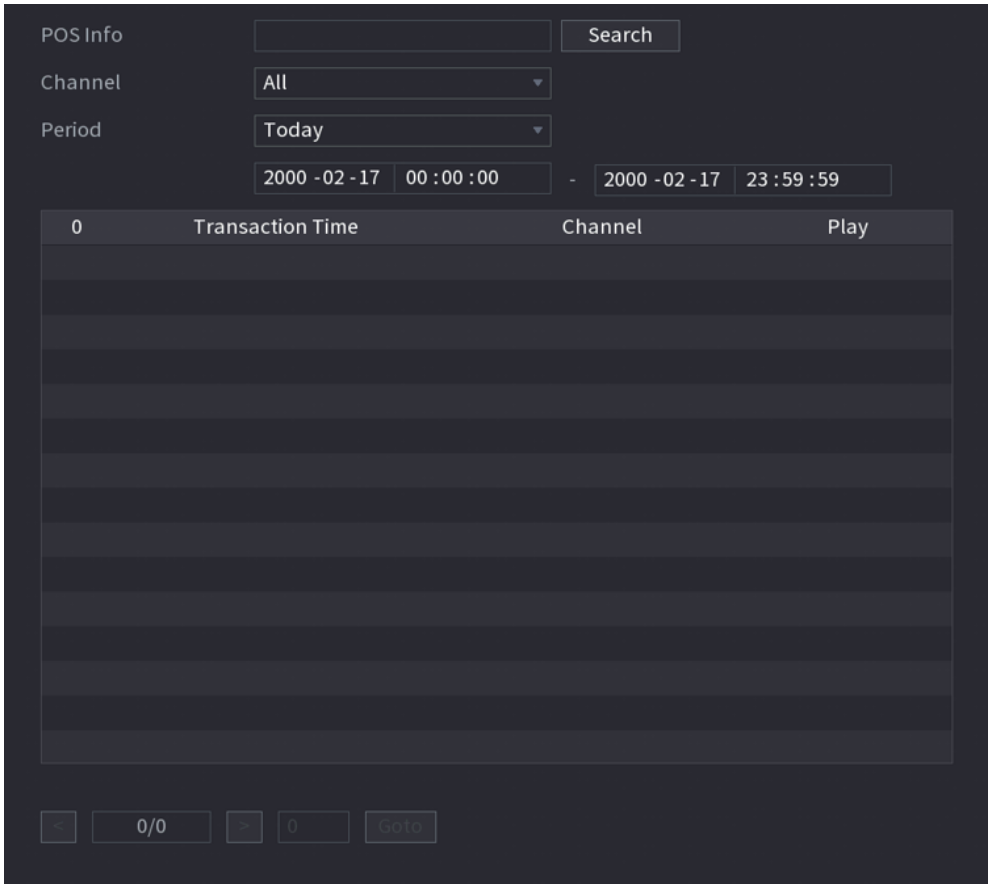
5.17.2 Search

The system supports fuzzy search.

Procedure

Step 1 Select **Main Menu** > **POS** > **POS Search**.

Figure 5-304 POS search



Step 2 In the **POS Search** box, enter the information such as transaction number on your receipt, amount, or product name.

Step 3 In the **Start Time** box and **End Time** box, enter the time period that you want to search the POS transaction information.

Step 4 Click **Search**.

The searched transaction results display in the table.

5.18 Audio

The audio function is to manage audio files and set schedule play function. It is to realize audio broadcast activation function.

This function is available on select models.

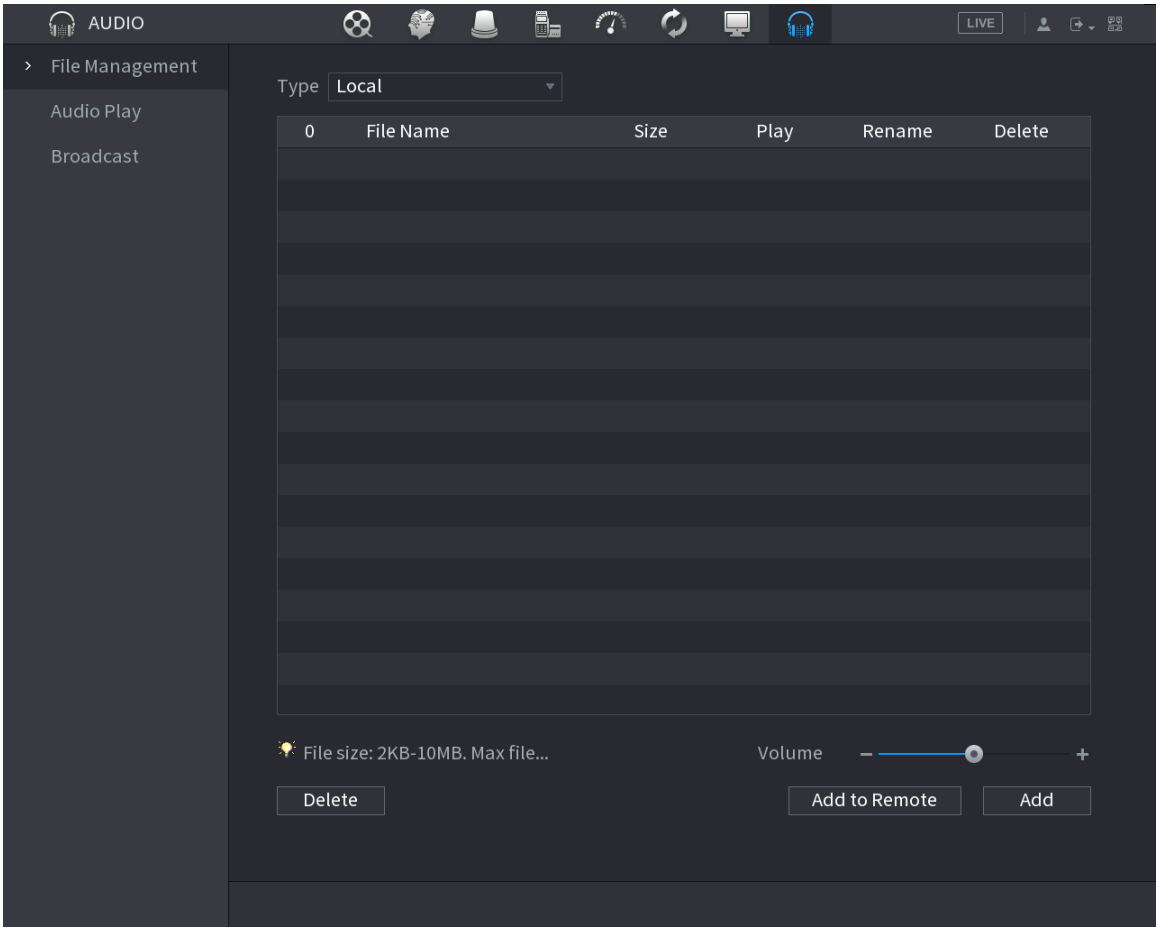
5.18.1 File Management

You can add audio files, listen to audio files, rename and delete audio files, and configure the audio volume.

Procedure

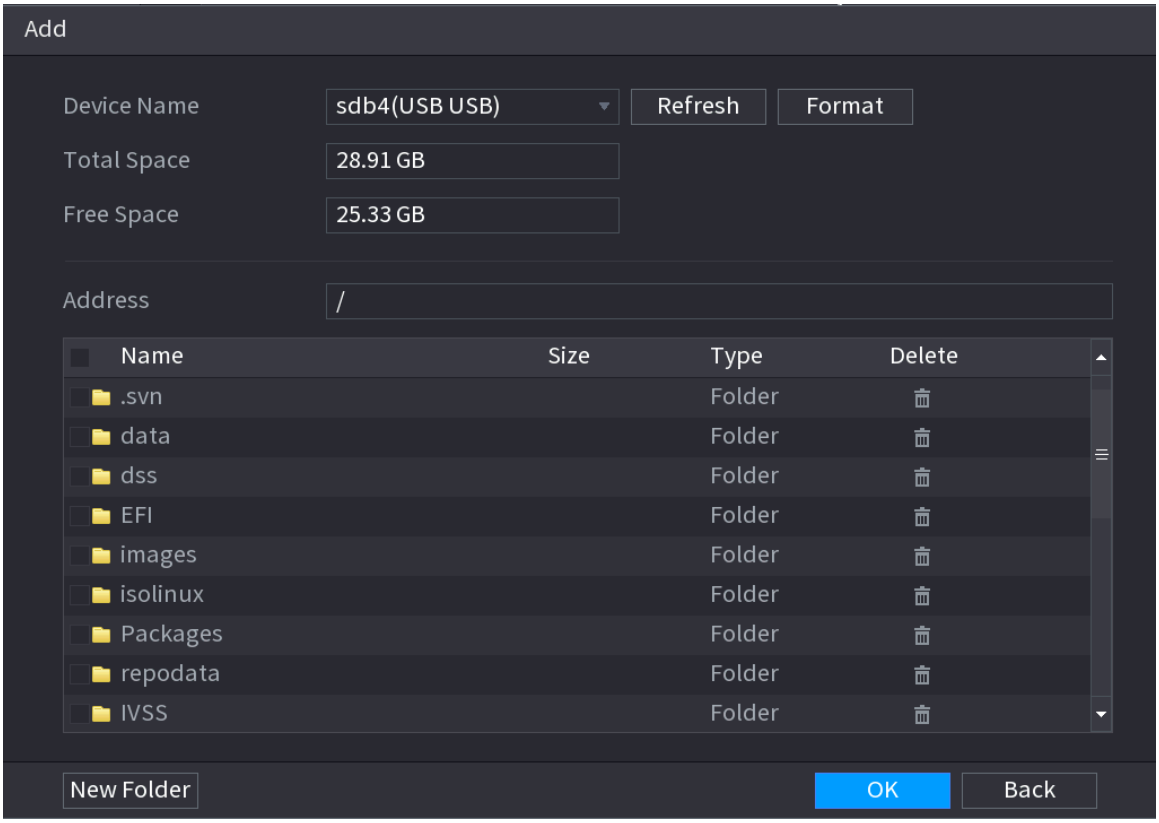
Step 1 Select **Main Menu** > **AUDIO** > **File Management**.

Figure 5-305 File management



Step 2 Click **Add**.

Figure 5-306 Add file



Step 3 Select the audio file and then click **Import**.

System supports MP3 and PCM audio format.

Step 4 Click **OK** to start importing audio files from the USB storage device.

If the importing is successful, the audio files will display in the **File Management** page.

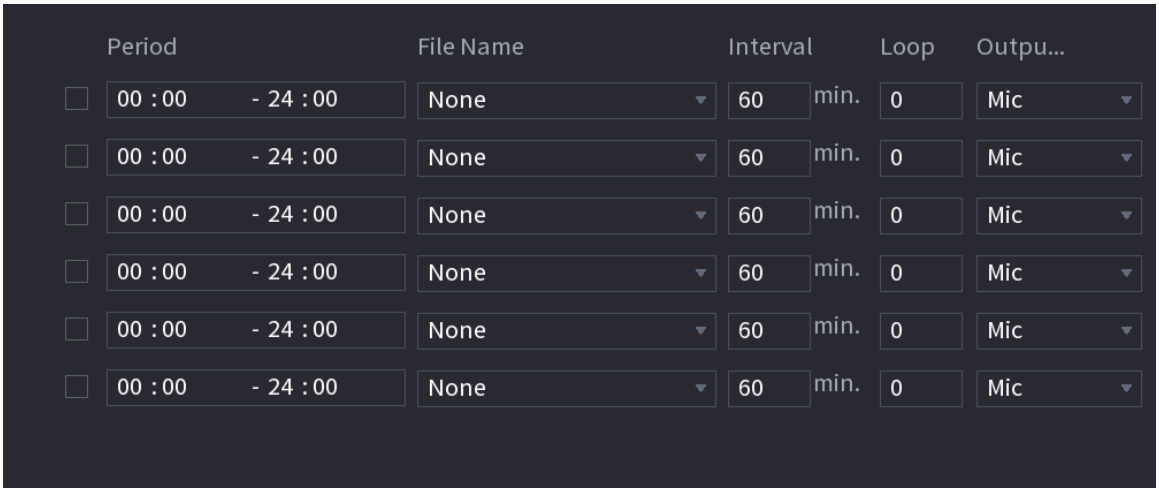
5.18.2 Audio Play

You can configure the settings to play the audio files during the defined time period.

Procedure

Step 1 Select **Main Menu** > **AUDIO** > **Schedule**.

Figure 5-307 Schedule



Step 2 Configure the parameters.

Table 5-89 Schedule parameters

Parameter	Description
Period	In the **Period** box, enter the time. Select the checkbox to enable the settings. You can configure up to six periods.
File Name	In the **File Name** list, select the audio file that you want to play for this configured period.
Interval	In the **Interval** box, enter the time in minutes for how often you want to repeat the playing.
Loop	Configure how many times you want to repeat the playing in the defined period.
Output	Includes two options: MIC and Audio. It is MIC by default. The MIC function shares the same port with talkback function and the latter has the priority. Some series products do not have audio port.

- The finish time for audio playing depends on audio file size and the configured interval.
- Playing priority: **Alarm event** > **Audio talk** > **Trial listening** > **Schedule audio file**.

Step 3 Click **Apply**.

5.18.3 Broadcast

System can broadcast to the camera, or broadcast to a channel group.

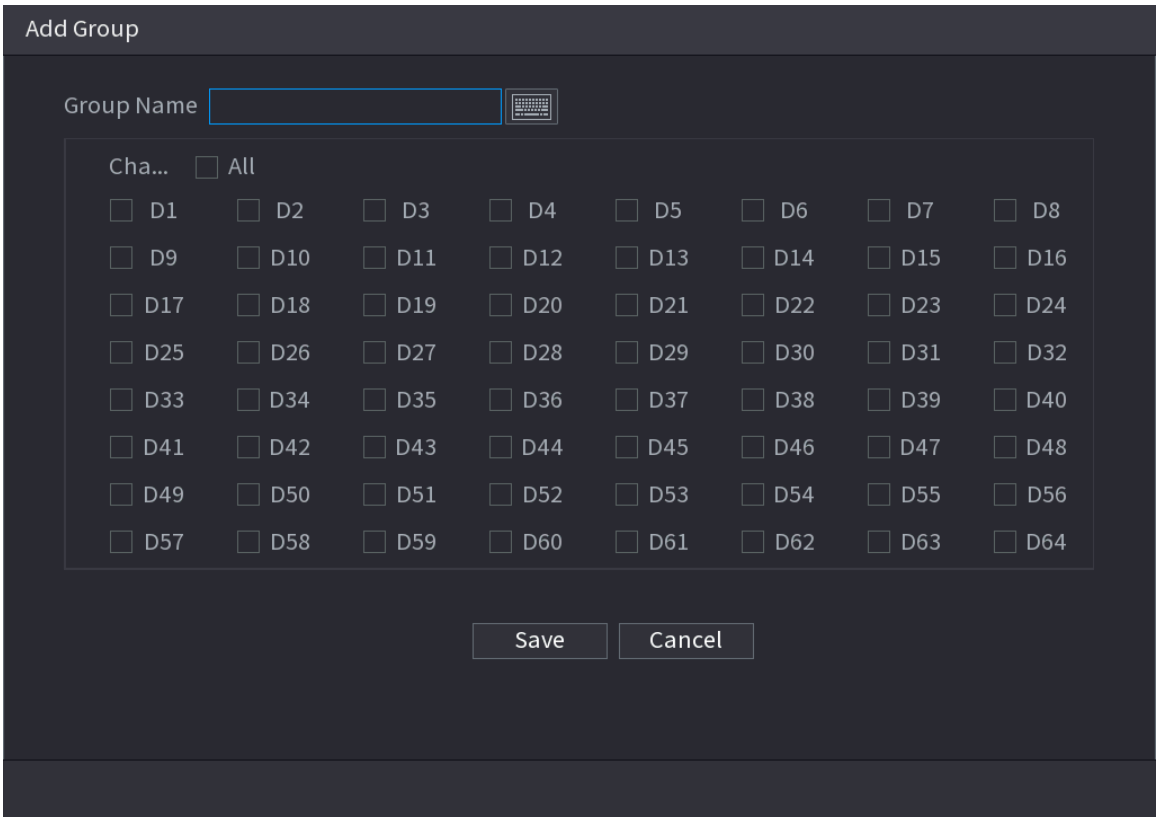
Procedure

Step 1 Select **Mani Menu** > **AUDIO** > **Broadcast**.

Figure 5-308 Broadcast

Step 2 Click **Add Group**.

Figure 5-309 Add group (1)

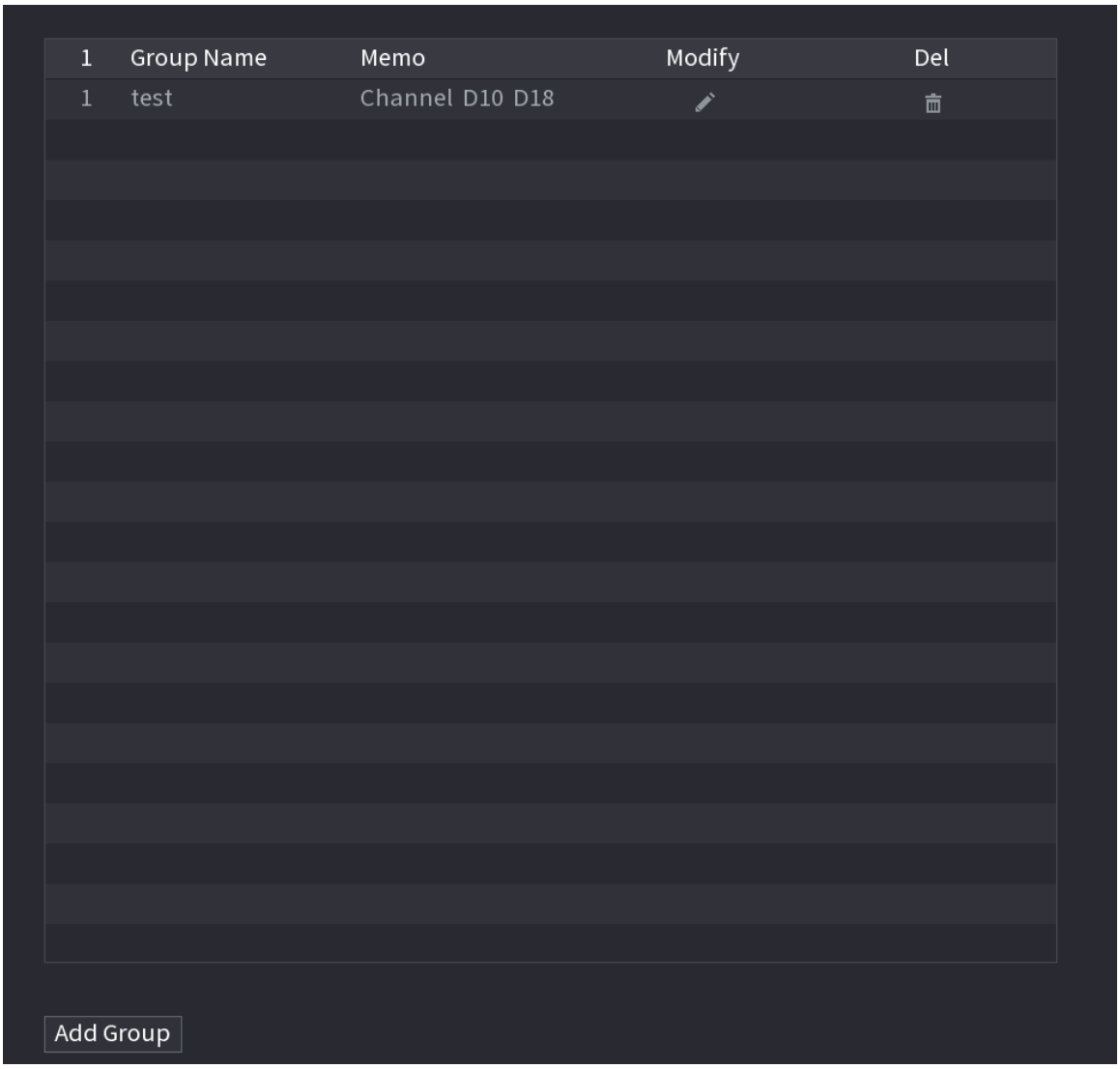


Step 3 Input group name and select one or more channels.

Step 4 Click **Save** to complete broadcast group setup.

- On the broadcast page, click to change group setup, click to delete group.
- After complete broadcast setup, on the preview page and then click on the navigation bar, device pops up broadcast dialogue box. Select a group name and then click to begin broadcast.

Figure 5-310 Add group (2)



5.19 Operation and Maintenance

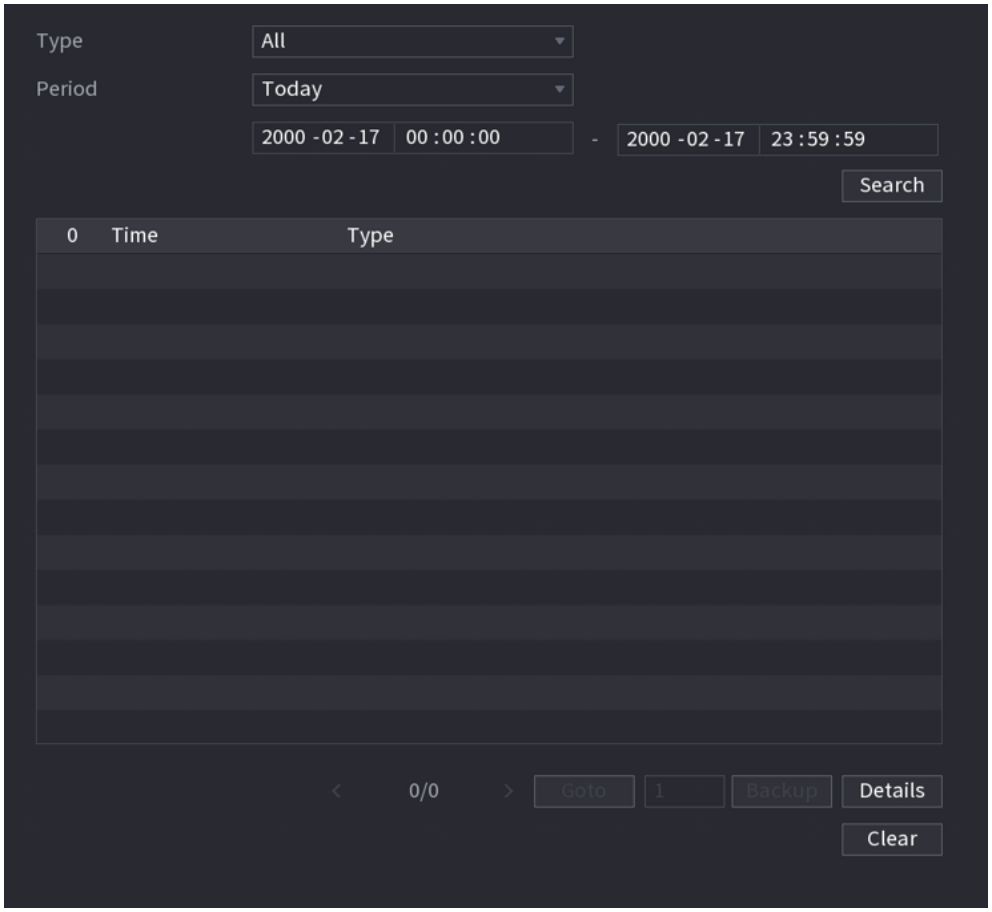
5.19.1 Log

You can view and search for the log information, or back up log to the USB device.

Procedure

Step 1 Select **Main Menu** > **Maintenance Center** > **Log**.

Figure 5-311 Log



Step 2 In the **Type** list, select the log type that you want to view (**System**, **Config**, **Storage**, **Record**, **Account**, **Clear Log**, **Playback**, and **Connection**) or select **All** to view all logs.

Step 3 Enter the time period to search, and then click **Search**.

The search results are displayed.

Related Operations

- Click **Details** or double-click the log to view details. Click **Next** or **Previous** to view more log information.
- Click **Backup** to back up the logs to the USB storage device.
- Click **Clear** to remove all logs.

5.19.2 System

5.19.2.1 System Version

Select **Main Menu** > **Maintenance Center** > **System Info** > **Version**.

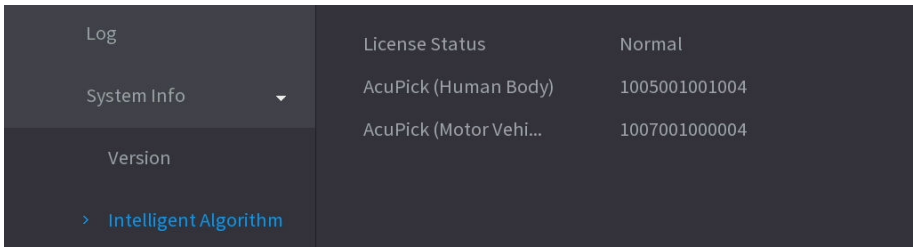
You can view NVR version information.

5.19.2.2 AI Algorithm Version

Select **Main Menu** > **Maintenance Center** > **System Info** > **Intelligent Algorithm**.

You can view version information for AI functions such as face detection, face recognition, IVS, and video metadata.

Figure 5-312 Intellifgent Algorithm



5.19.2.3 HDD Info

You can view the HDD quantity, HDD type, total space, free space, status, and S.M.A.R.T information.

Select **Main Menu** > **Maintenance Center** > **System Info** > **Disk**.

Figure 5-313 Disk information

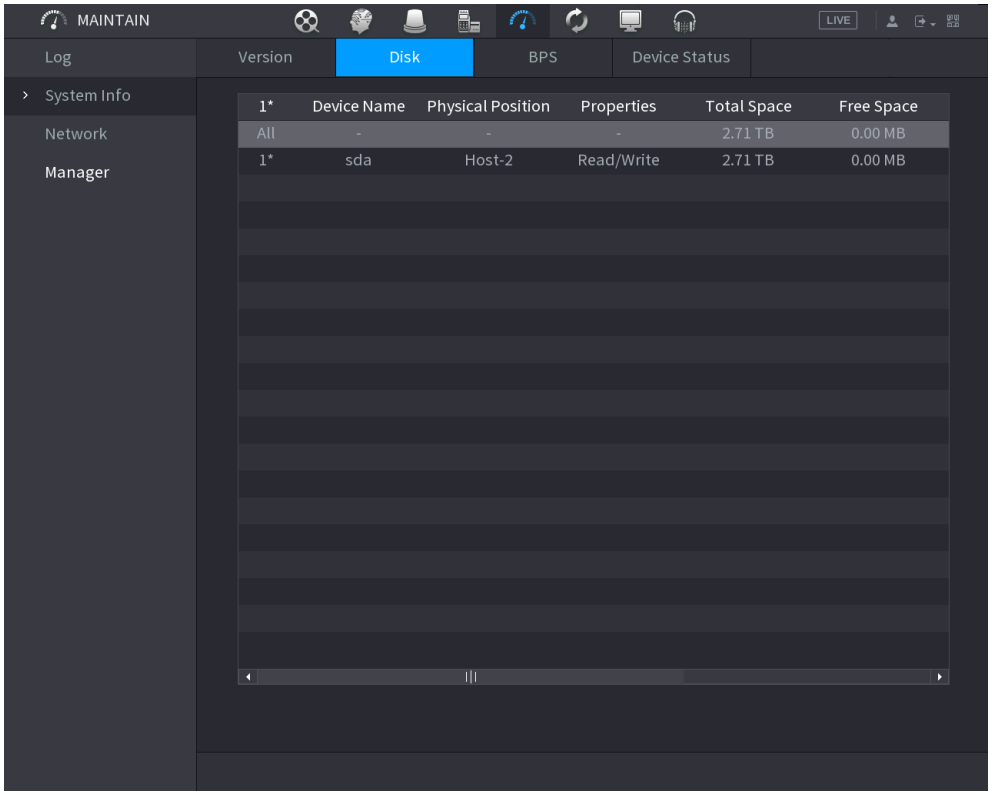


Table 5-90 Disk information

Parameter	Description
No.	Indicates the number of the currently connected HDD. The asterisk (*) means the current working HDD.
Device Name	Indicates name of HDD.
Physical Position	Indicates installation position of HDD.
Properties	Indicates HDD type.

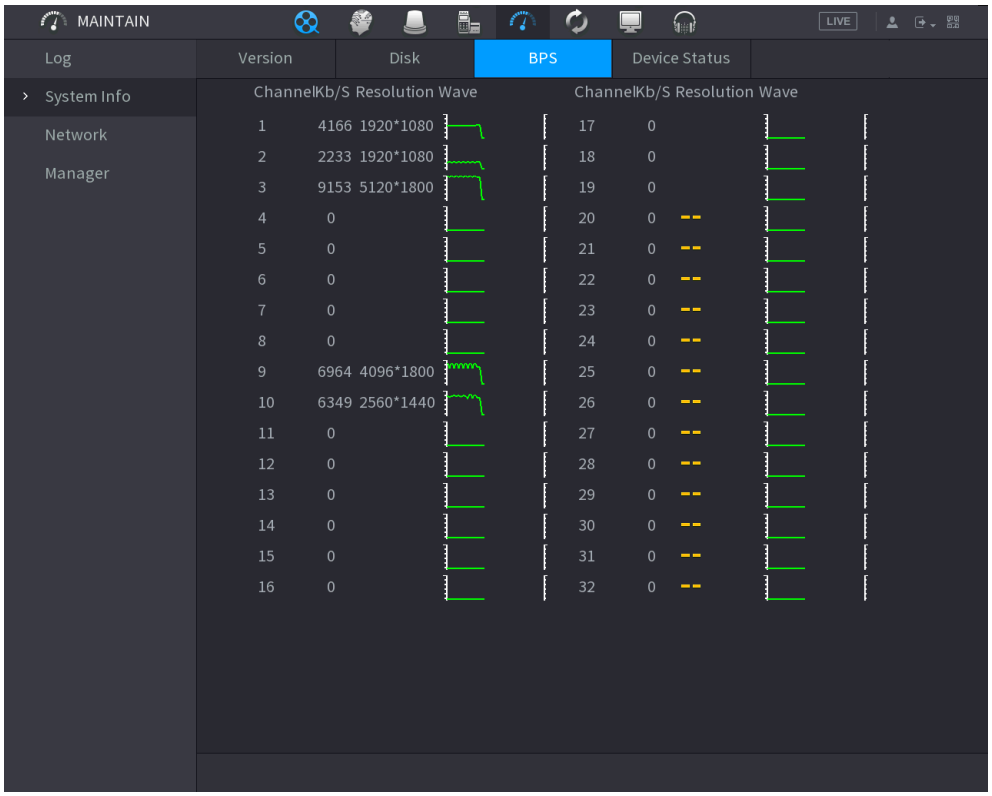
Parameter	Description
Total Space	Indicates the total capacity of HDD.
Free Space	Indicates the usable capacity of HDD.
Health Status	Indicates the health status of the HDD.
S.M.A.R.T	View the S.M.A.R.T reports from HDD detecting.
Status	Indicates the status of the HDD to show if it is working normally.

5.19.2.4 BPS

You can view current video bit rate (kb/s) and resolution.

Select **Main Menu** > **Maintenance Center** > **System Info** > **BPS**.

Figure 5-314 BPS

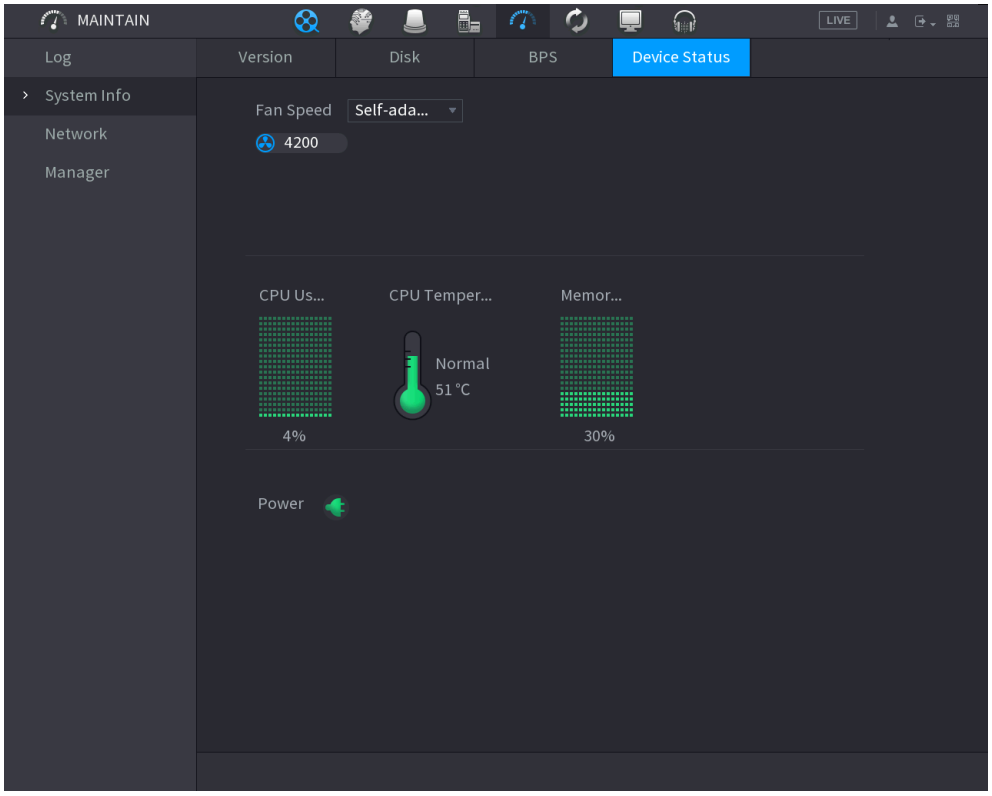


5.19.2.5 Device Status

You can view fan running status such as speed, CPU temperature, and memory.

Select **Main Menu** > **Maintenance Center** > **System Info** > **Device Status**.

Figure 5-315 Device status



5.19.3 Network

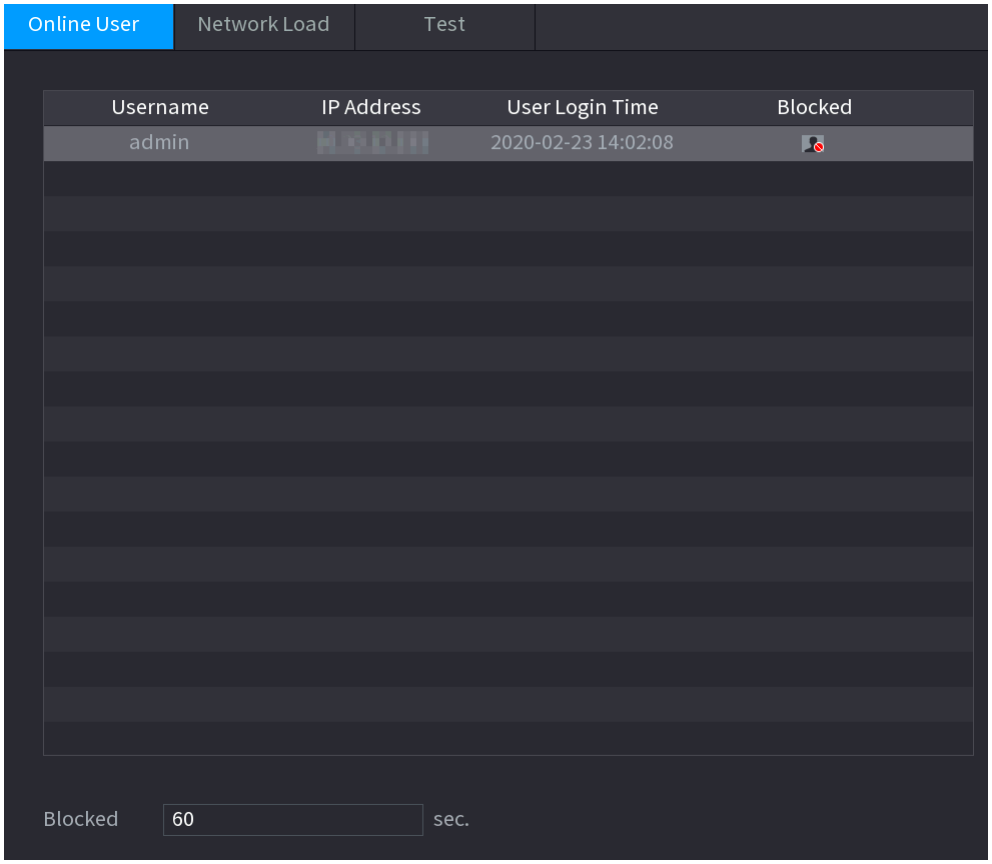
5.19.3.1 Online User

You can view the online user information or block any user for a period of time. To block an online user, click and then enter the time that you want to block this user. The maximum value you can set is 65535.

The system detects every 5 seconds to check whether there is any user added or deleted, and update the user list timely.

Select **Main Menu** > **Maintenance Center** > **Network** > **Online User**.

Figure 5-316 Online user



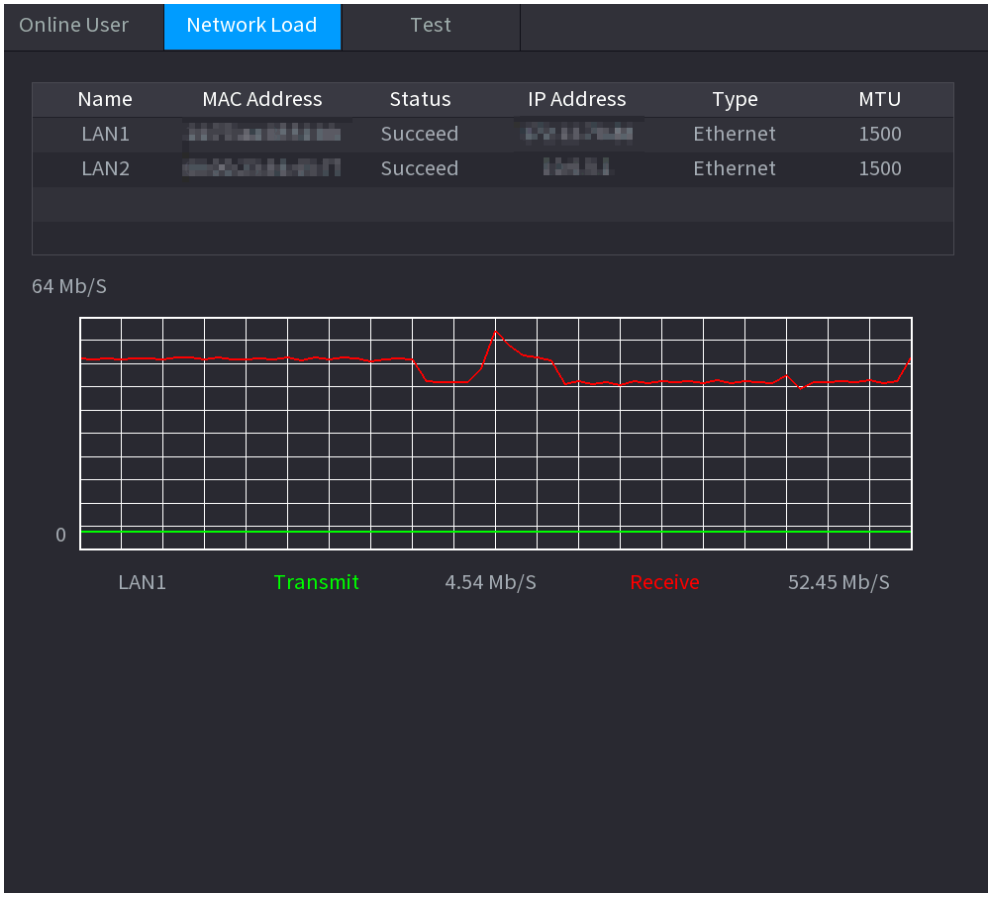
5.19.3.2 Network Load

Network load means the data flow which measures the transmission capability. You can view the information such as data receiving speed and sending speed.

Procedure

Step 1 Select **Main Menu** > **Maintenance Center** > **Network** > **Network Load**.

Figure 5-317 Network load



Step 2 Click the LAN name that you want to view, for example, **LAN1**.

The system displays the information of data sending speed and receiving speed.

- System displays LAN1 load by default.
- Only one LAN load can be displayed at one time.

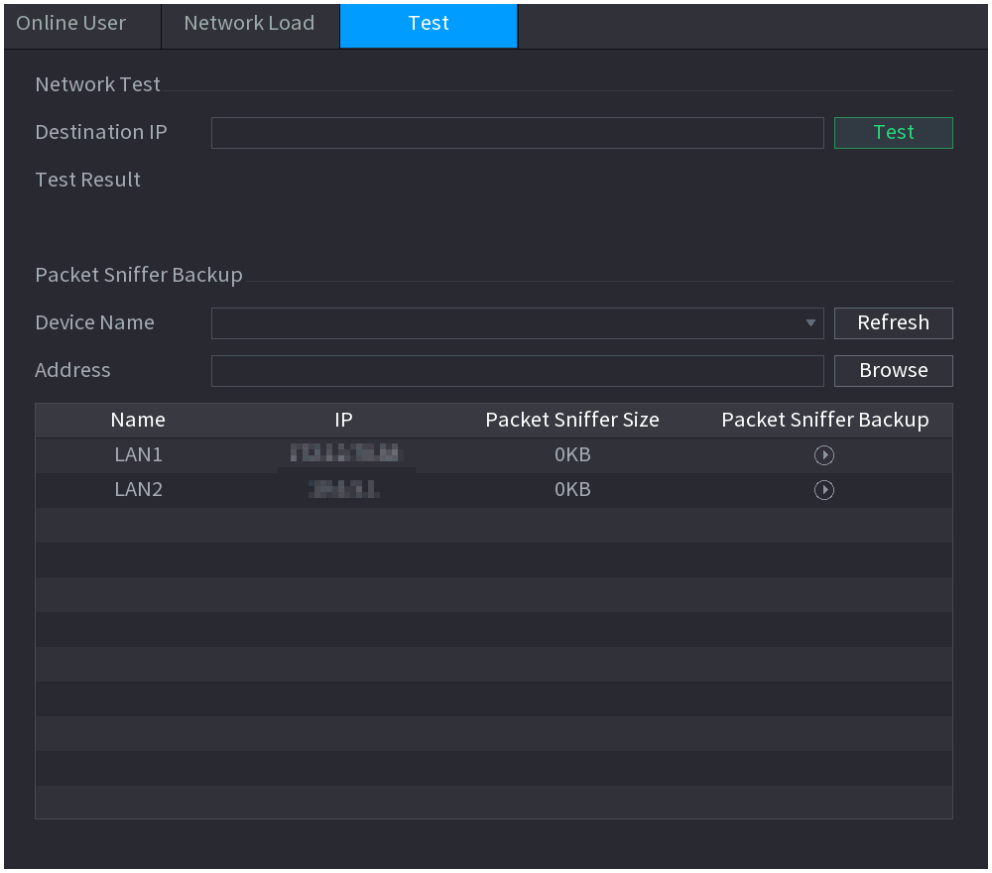
5.19.3.3 Network Test

You can test the network connection status between the Device and other devices.

Procedure

Step 1 Select **Main Menu** > **Maintenance Center** > **Network** > **Test**.

Figure 5-318 Test



Step 2 In the **Destination IP** box, enter the IP address.

Step 3 Click **Test**.

After testing is completed, the test result is displayed. You can check the evaluation for average delay, packet loss, and network status.

5.19.4 Maintenance and Management

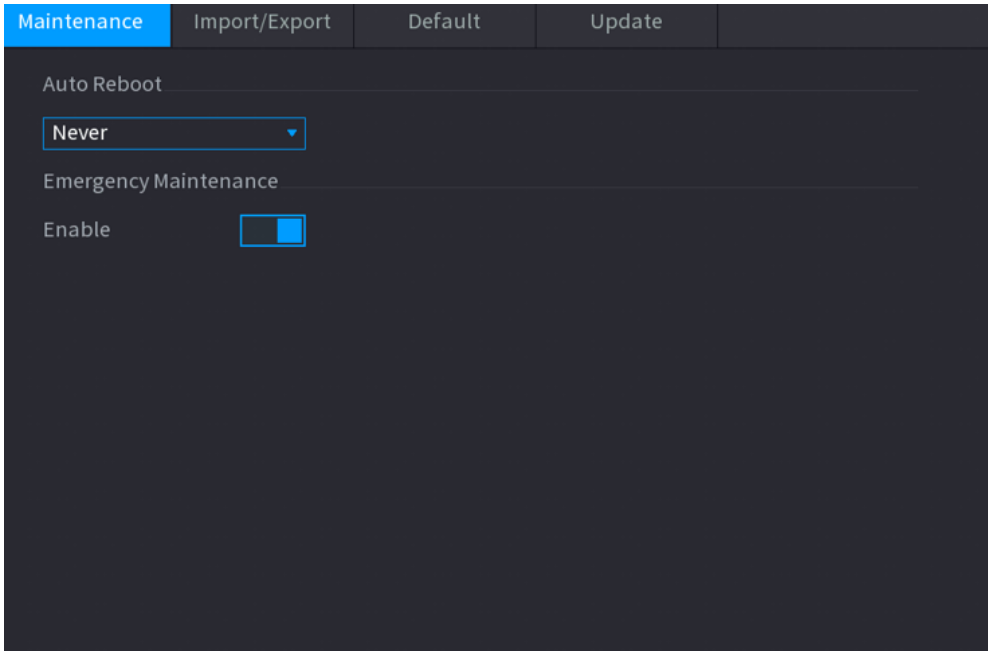
5.19.4.1 Device Maintenance

When the Device has been running for a long time, you can enable the Device to restart automatically at the idle time. You can also enable emergency maintenance.

Procedure

Step 1 Select **Main Menu** > **Maintenance Center** > **Manager** > **Maintenance**.

Figure 5-319 Maintenance



Step 2 Configure the parameters.

- **Auto Reboot** : Enable the Device to restart at the idle time.
- **Emergency Maintenance** : When the Device has an update power outage, running error and other problems, and you cannot log in, then you can use the emergency maintenance function to restart the Device, clear configuration, update the system, and more.

Step 3 Click **Apply**.

5.19.4.2 Exporting System Settings

Background Information

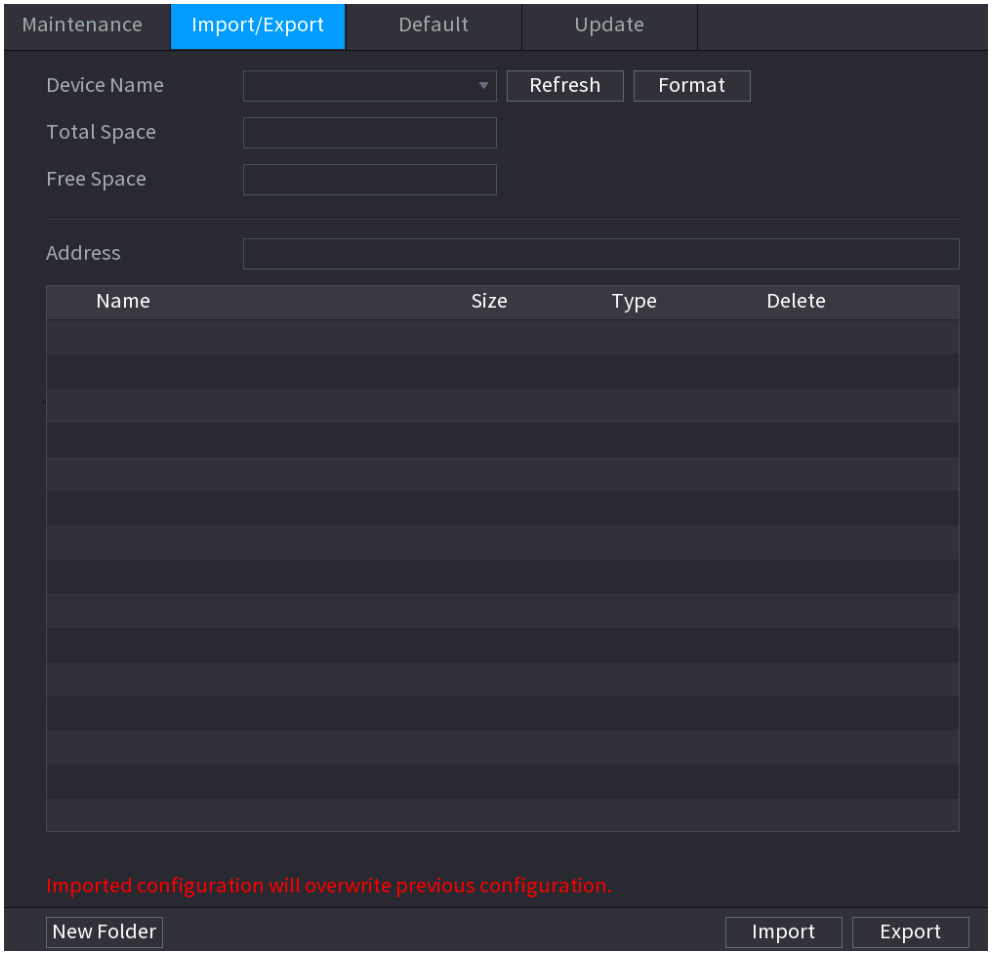
You can export or import the Device system settings if there are several Devices that require the same setup.

- The **Import/Export** page cannot be opened if the backup operation is ongoing on the other pages.
- When you open the **Import/Export** page, the system refreshes the devices and sets the current directory as the first root directory.
- Click **Format** to format the USB storage device.

Procedure

Step 1 Select **Main Menu** > **Maintenance Center** > **Manager** > **Import/Export**.

Figure 5-320 Import and export

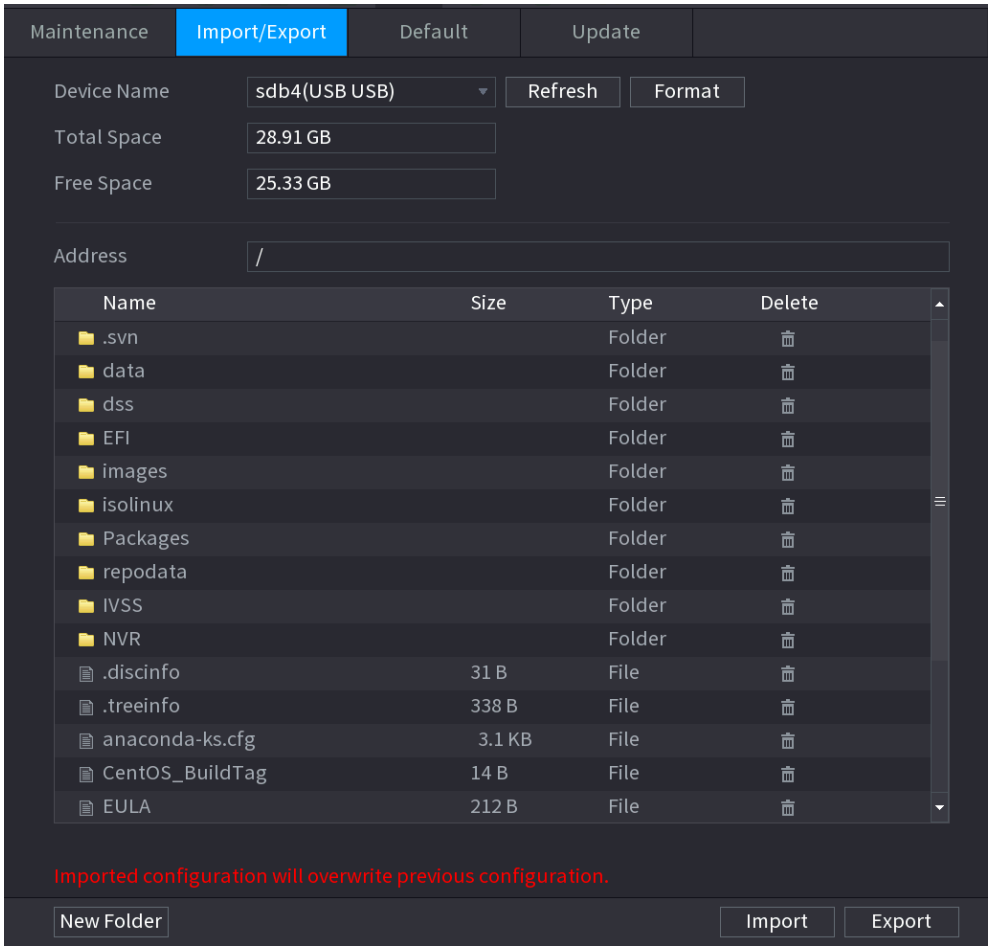


Step 2 Insert a USB storage device into one of the USB ports on the Device.

Step 3 Click **Refresh** to refresh the page.

The connected USB storage device is displayed.

Figure 5-321 Connected USB device



Step 4 Click **Export**.

There is a folder under the name style of "Config_xxxx". Double-click this folder to view the backup files.

5.19.4.3 Restoring Defaults

5.19.4.3.1 Restoring Defaults on the Local Page

Background Information

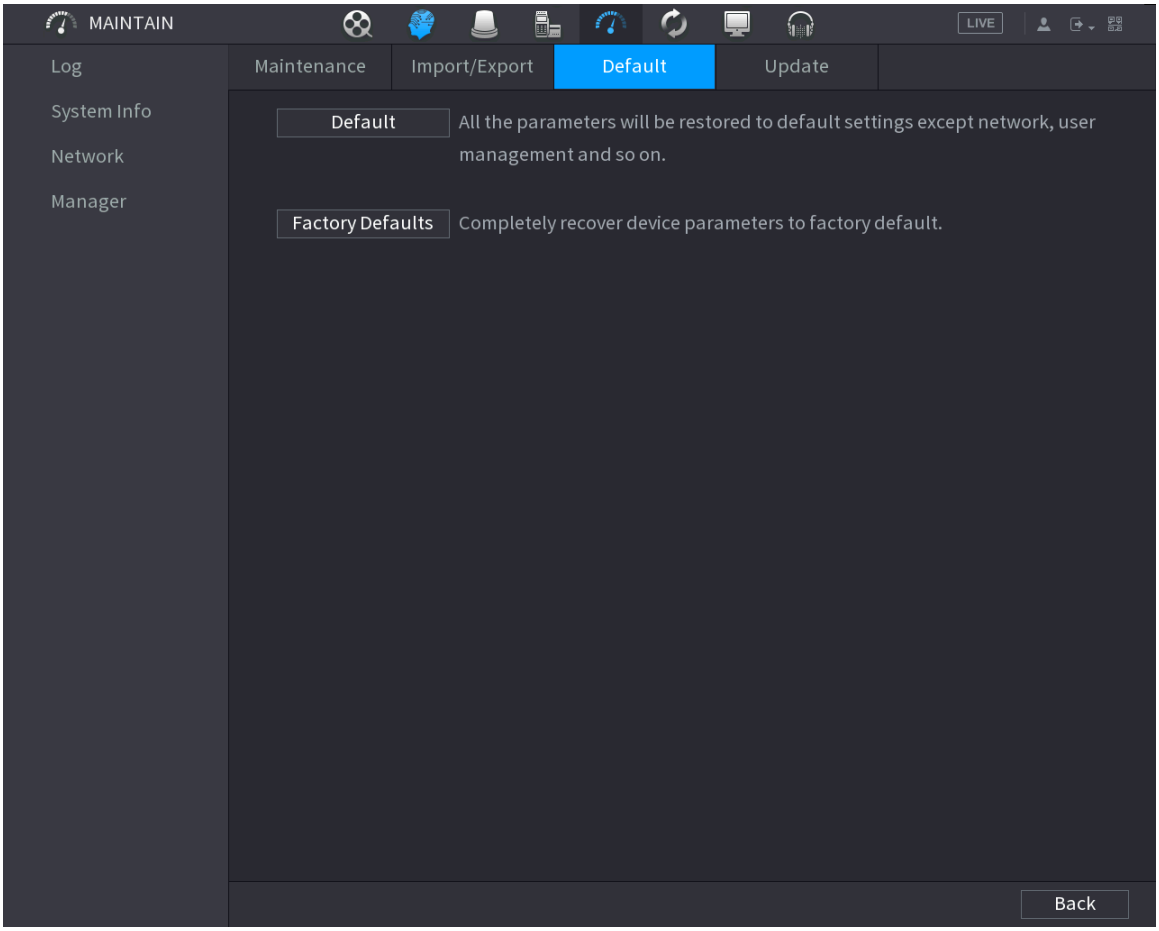
This function is for admin account only.

You can restore the Device to default settings on the local page.

Procedure

Step 1 Select **Main Menu** > **Maintenance Center** > **Manager** > **Default**.

Figure 5-322 Default



Step 2 Restore the settings.

- **Default**: Restore all the configurations except network settings and user management to the default.
- **Factory Default**: Restore all the configurations to the factory default settings.

5.19.4.3.2 Resetting Device through the Reset Button

Background Information

You can use the reset button on the mainboard to reset the Device to the factory default settings.

After resetting, all the configurations will be lost.

The reset button is available on select models.

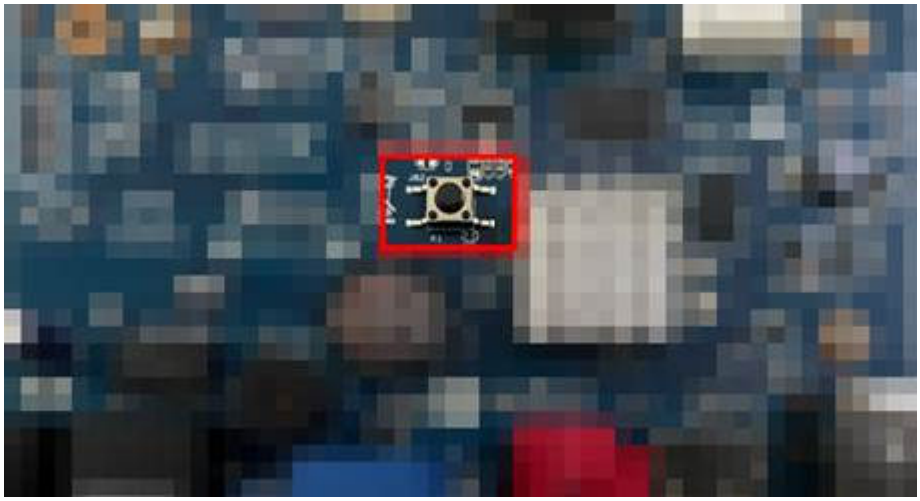
Procedure

Step 1 Disconnect the Device from power source, and then remove the cover panel. For details about removing the cover panel, see "3.3 HDD Installation".

Step 2 Find the reset button on the mainboard, and then connect the Device to the power source again.

Step 3 Press and hold the reset button for 5 seconds to 10 seconds.

Figure 5-323 Reset button



Step 4 Restart the Device.

After the Device restarts, the settings have been restored to the factory default.

5.19.4.4 System Update

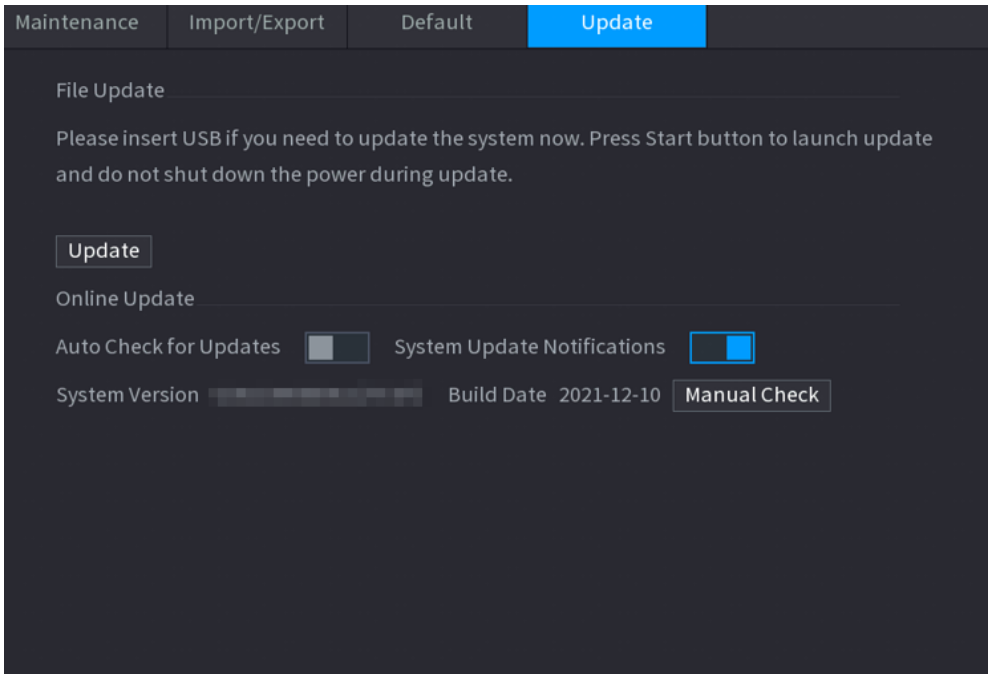
5.19.4.4.1 Upgrading File

Procedure

Step 1 Insert a USB storage device containing the upgrade files into the USB port of the Device.

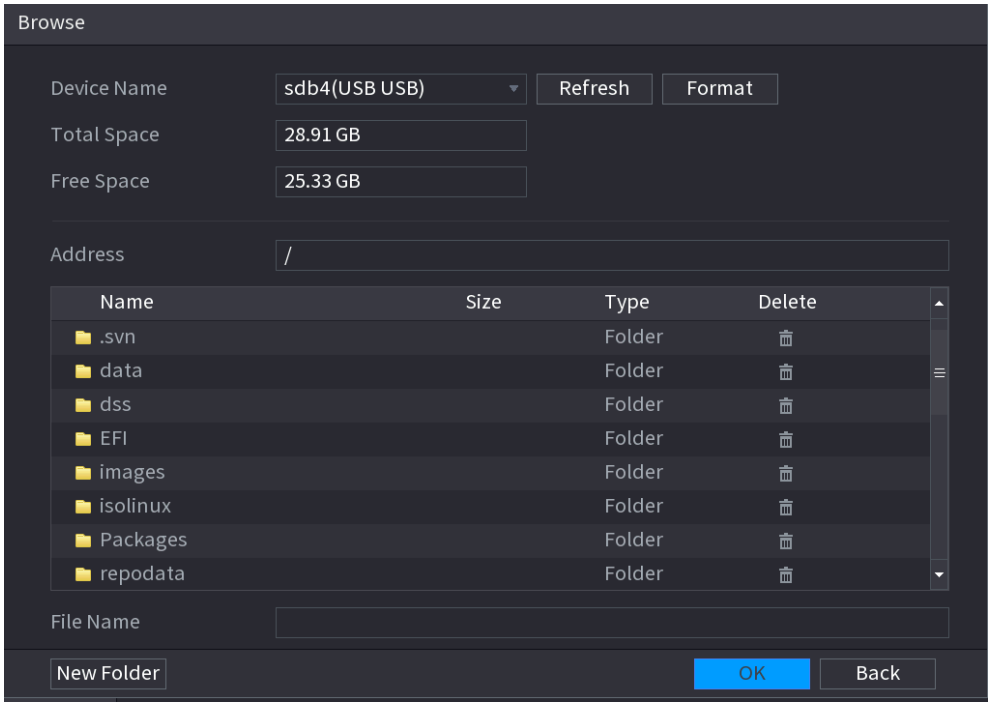
Step 2 Select **Main Menu** > **Maintenance Center** > **Manager** > **Update**

Figure 5-324 Update



Step 3 Click **Update**.

Figure 5-325 Browse



Step 4 Click the file that you want to upgrade.

Step 5 The selected file is displayed in the **Update File** box.

Step 6 Click **Start**.

5.19.4.4.2 Online Upgrade

Background Information

When the Device is connected to Internet, you can use online upgrade function to upgrade the system.

Before using this function, you need to check whether there is any new version by auto check or manual check.

- Auto check: The Device checks if there is any new version available at intervals.
- Manual check: Perform real-time check whether there is any new version available.

Ensure the correct power supply and network connection during upgrading; otherwise the upgrading might be failed.

Procedure

Step 1 Select **Main Menu** > **Maintenance Center** > **Manager** > **Update**.

Step 2 Check whether there is any new version available.

- Auto-check for updates: Enable Auto-check for updates.
- Manual check: Click **Manual Check**.

The system starts checking the new versions. After checking is completed, the check result is displayed.

- If the "It is the latest version" text is displayed, you do not need to upgrade.
- If the text indicating there is a new version, go to the step 3.

Step 3 Click **Update now** to update the system.

5.19.4.4.3 Uboot Upgrading

- Under the root directory in the USB storage device, there must be "u-boot.bin.img" file and "update.img" file saved, and the USB storage device must be in FAT32 format.
- Make sure the USB storage device is inserted; otherwise the upgrading cannot be performed.

When starting the Device, the system automatically checks whether there is a USB storage device connected and any upgrade file, and if yes and the check result of the upgrade file is correct, the system will upgrade automatically. The Uboot upgrade can avoid the situation that you have to upgrade through +TFTP when the Device is halted.

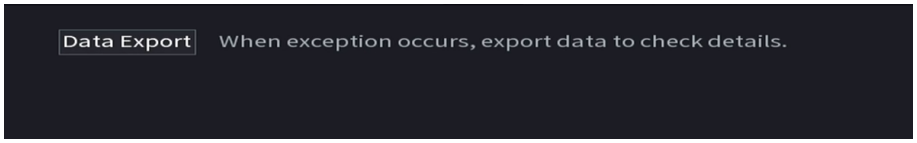
5.19.4.5 Intelligent Diagnosis

When exception occurs, export data to check details

Background Information

Select **Maintenance Center** > **Intelligent Diagnosis**.

Figure 5-326 Intelligent diagnosis

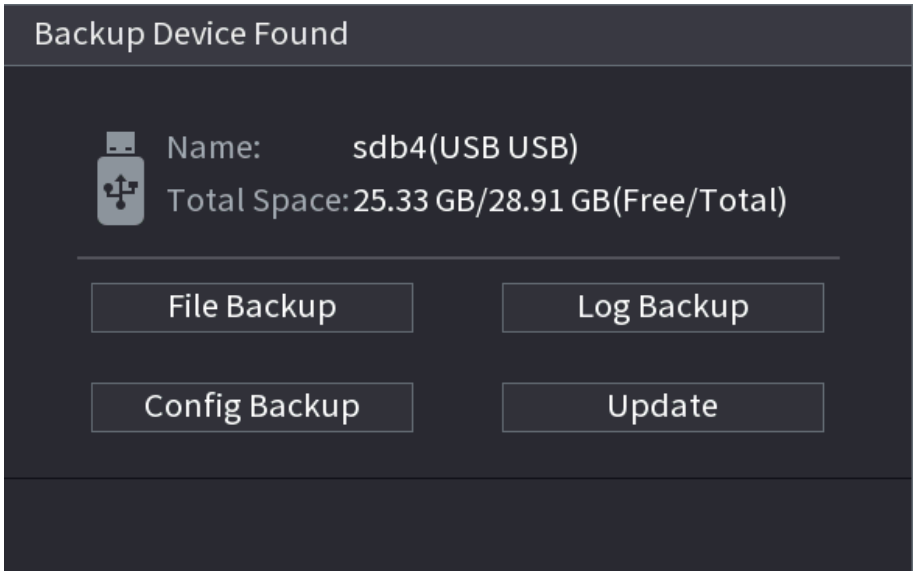


5.20 USB Device Auto Pop-up

After you inserted the USB device, system can auto detect it and pop up the following dialogue box. It allows you to conveniently backup file, log, configuration or update system.

You can add a USB keyboard through USB port, and it can input characters limited to soft keyboard.

Figure 5-327 USB device prompt



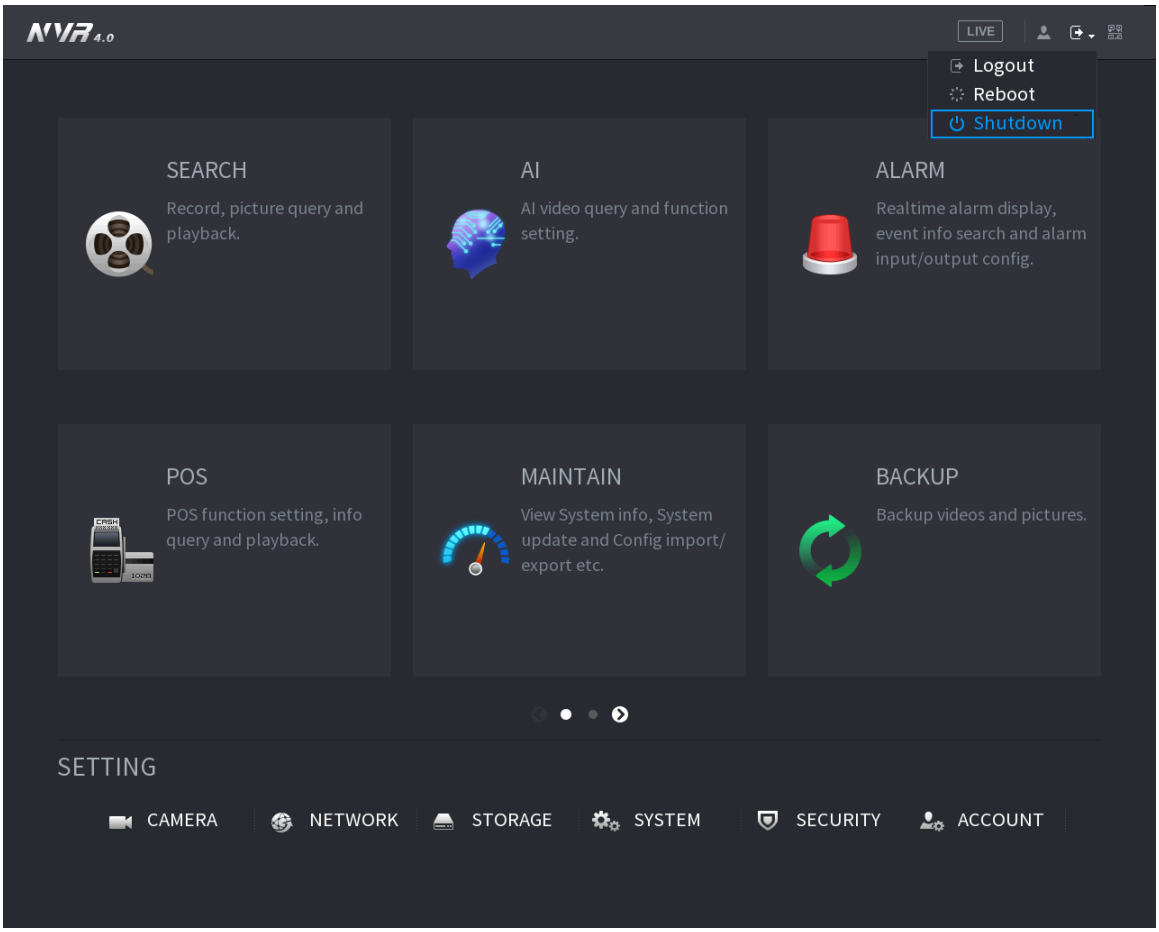
5.21 Shutdown

- When you see corresponding dialogue box "System is shutting down…" Do not click power on-off button directly.
- Do not unplug the power cable or click power on-off button to shutdown device directly when device is running (especially when it is recording.)
- Shut down the device and then unplug the power cable before you replace the HDD.

Procedure

- From the main menu (Recommended)
  1. Click at the upper-right corner.

Figure 5-328 Shutdown (1)



2. Select **Shutdown.**

   Draw the unlock pattern or input password first if you have no authority to shut down.

Figure 5-329 Shutdown (2)

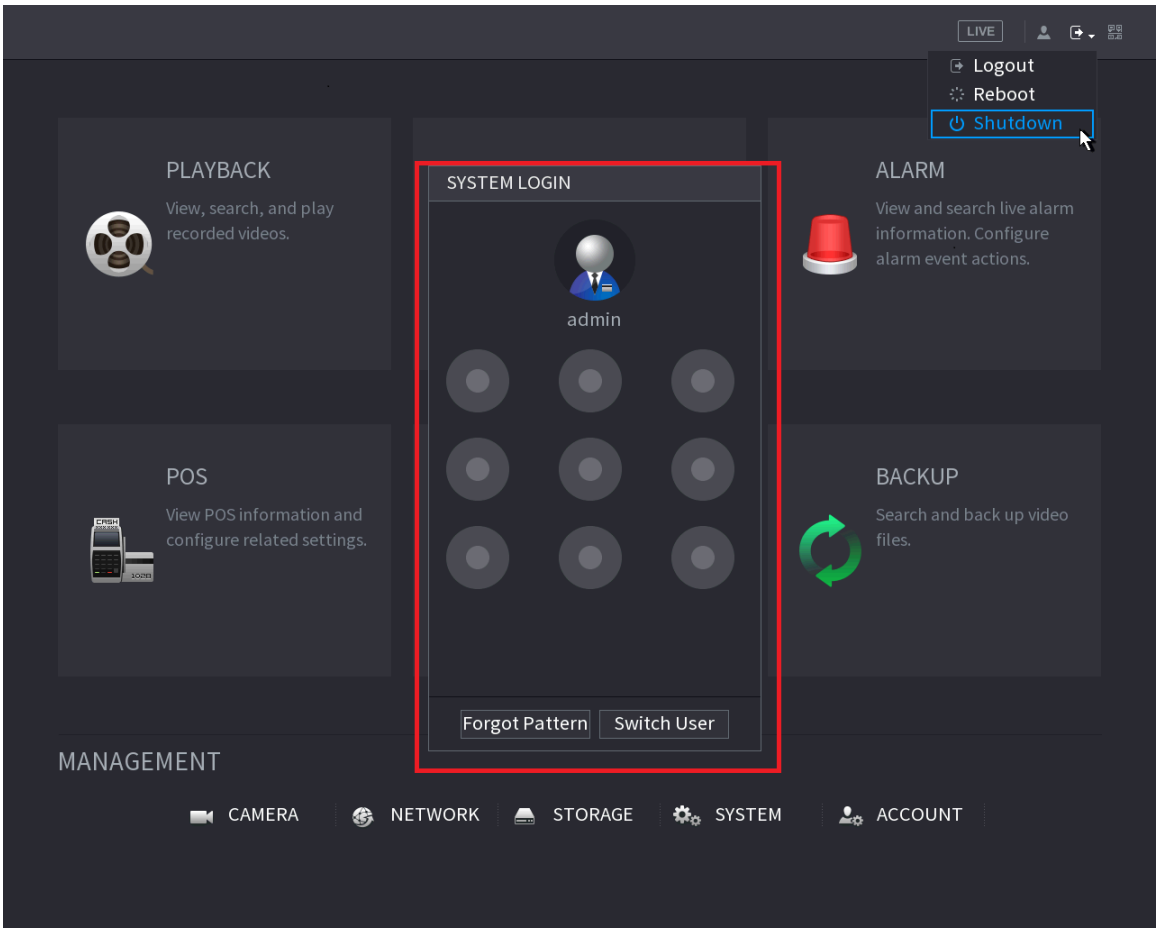
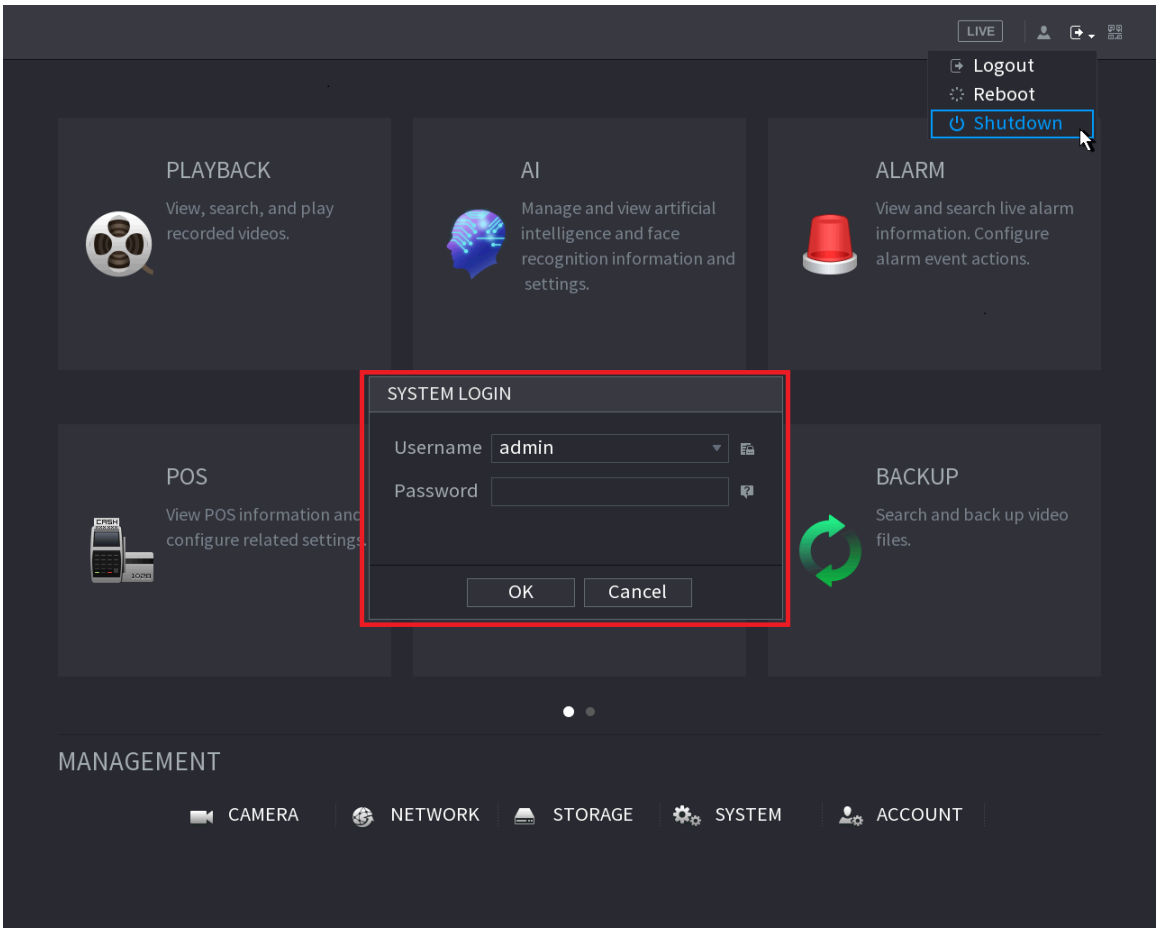


Figure 5-330 Shutdown (3)



- Remote Control

  Press the power button on the remote for at least 3 seconds.
- Press the power button at the rear panel of the device.

Auto Resume after Power Failure

The system can automatically backup video file and resume previous working status after power failure.

6 Web Operation

- The figures in the Manual are used for introducing the operations and only for reference. The actual page might be different dependent on the model you purchased.
- The Manual is a general document for introducing the product, so there might be some functions described for the Device in the Manual not apply to the model you purchased.
- Besides Web, you can use our Smart PSS to login the device. For detailed information, see Smart PSS user's manual.

6.1 Network Connection

Background Information

- The factory default IP of the Device is 192.168.1.108.
- The Device supports monitoring on different browsers such as Safari, Firefox, Google to perform the functions such as multi-channel monitoring, PTZ control, and device parameters configurations.

Procedure

Step 1 Check to make sure the Device has connected to the network.

Step 2 Configure the IP address, subnet mask and gateway for the PC and the Device. For details about network configuration of the Device, see "5.19.3 Network".

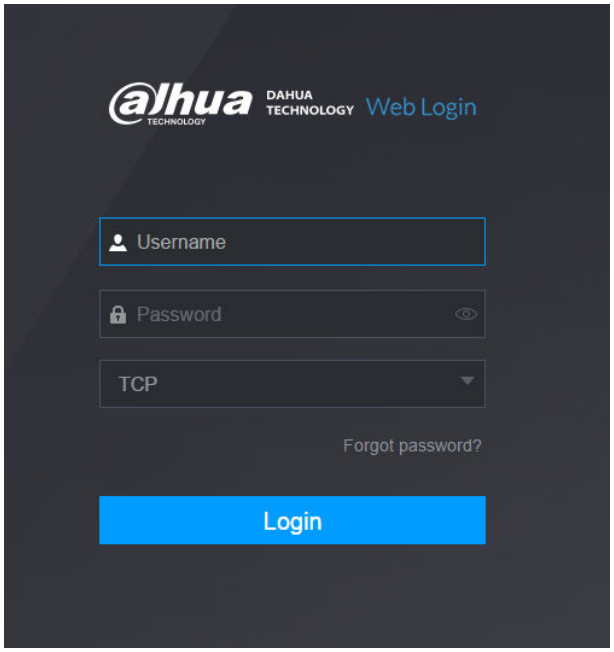
Step 3 On your PC, check the network connection of the Device by using "ping ***.***.***.***". Usually the return value of TTL is 255.

6.2 Web Login

Procedure

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

Figure 6-1 Login



Step 2 Enter the username and password.

- The default administrator account is **admin**. The password is the one that was configured during initial settings. To ensure your account security, we recommend you keep the password properly and change it regularly.
- Click to display the password.

Step 3 Click **Login**.

6.3 Web Main Menu

After you have logged in to the web, the main menu is displayed.

For detailed operations, see "5 Local Operations".

Figure 6-2 Main menu

Table 6-1 Main menu symbols

No.	Icon	Description
1		Includes configuration menu through which you can configure camera settings, network settings, storage settings, system settings, account settings, and view information.
2	None	Displays system date and time.
3		When you point to , the current user account is displayed.
4		Click , select Logout, Reboot, or Shutdown according to your actual situation.
5		Displays Cell Phone Client and Device SN QR Code. • Cell Phone Client: Use your mobile phone to scan the QR code to add the device into the Cell Phone Client, and then you can start accessing the Device from your cell phone. • Device SN: Obtain the Device SN by scanning the QR code. Go to the P2P management platform and add the Device SN into the platform. Then you can access and manage the device in the WAN. For details, see the P2P operation manual. You can also configure P2P function in the local configurations, see "5.11.18 P2P".
6		Displays the web main menu.

No.	Icon	Description
7	None	Includes eight function tiles: **LIVE, PLAYBACK, AI, ALARM, POS, OPERATION, BACKUP, DISPLAY, and AUDIO**. Click each tile to open the configuration page of the tile. • **LIVE**: You can perform the operations such as viewing real-time video, configuring channel layout, setting PTZ controls, and using smart talk and instant record functions if needed. • **PLAYBACK**: Search for and play back the recorded video saved on the Device. • **ALARM**: Search for alarm information and configure alarm event actions. • **AI**: Configure and manage artificial intelligent events. It includes smart search, parameters, and database. • **POS**: View POS information and configure related settings. • **OPERATION**: View system information, import/export system configuration files, or update system. • **BACKUP**: Search and back up the video files to the local PC or external storage device such as USB storage device. • **DISPLAY**: Configure the display effect such as displaying content, image transparency, and resolution, and enable the zero-channel function. • **AUDIO**: Manage audio files and configure the playing schedule. The audio file can be played in response to an alarm event if the voice prompts function is enabled.

6.4 Cluster Service

The cluster function, also known as cluster redundancy, is a kind of deployment method that can improve the reliability of the device. In the cluster system, there is a number of main devices and another number of sub devices (the N+M mode), and they have a virtual IP address (the cluster IP). When the main device fails, the corresponding sub device will take over the job automatically. When the main device recovers, the sub device will transmit the configuration data, cluster IP address and videos recorded during the failure to the main device which then takes over the job again.

In the N+M cluster system, there is a management server, the DCS (Dispatching Console) server, which is responsible for timely and correct scheduling management of the main and sub devices. When you create a cluster, the current device is used as the first sub device and the DCS server by default.

This function is available on select models.

6.4.1 Configuring Cluster IP

When the main device malfunctions, the sub device can use the main device configuration and virtual IP address to replace the work (monitor or record) accordingly. When you use the virtual IP to access the device, you can still view the real-time video and there is no risk of record loss.

Procedure

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

Step 2 Select **SETTING** > **Cluster Service** > **CLUSTER IP**.

Step 3 Select **Enable**.

Step 4 Configure **IP Address** , **Subnet Mask** and **Default Gateway**.

Step 5 Click **OK**.

6.4.2 Main Device

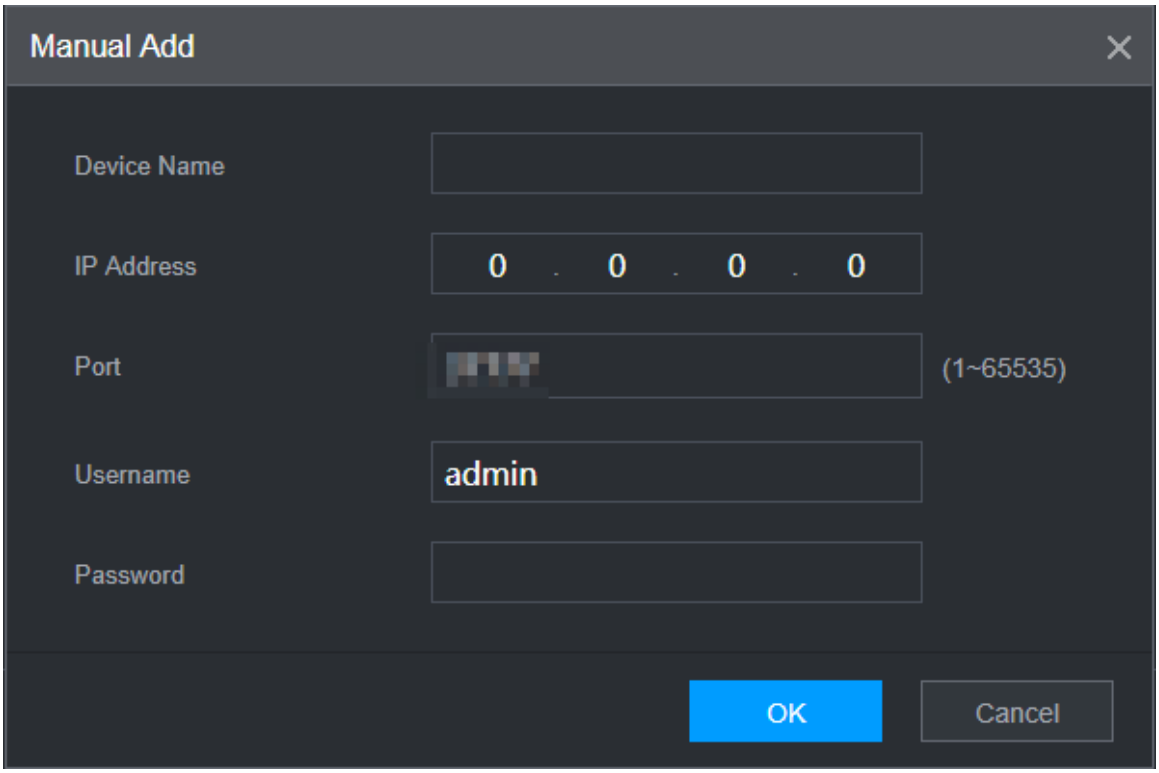
You can add several main devices manually. After you enable the cluster function, you can vie IP address, working status and connection log of the main device.

Procedure

Step 1 Select **SETTING** > **Cluster Service** > **Main Device**.

Step 2 Click **Manual Add**.

Figure 6-3 Manual add



Step 3 Configure parameters.

Table 6-2 Parameters of adding main device

Parameter	Description
Device Name	Customize the device name.
IP Address	Enter the IP address of the NVR.
Port	Set the TCP port number of the server. The default value is 37777. You can view the current TCP port number in **SETTING** > **Network** > **Port**.
Username/Password	Enter the username and password of the NVR.

Step 4 Click **OK**.

Step 5 (Optional) Click to view event occurrence time, name, operation and reason.

6.4.3 Sub Device

Background Information

When you add the first sub device, the default IP is the device IP address that logs in on the web.

From **SETTING** > **Cluster Service** > **Sub Device**, you can add sub devices. For details, see "6.4.2 Main Device".

When adding the first sub device, you need not enter the IP address, because the first sub device is the current device by default.

After you added main device and sub device, you need to enable cluster function. See "6.4.5 Configuring Cluster Control" for more information.

6.4.4 Transferring Videos

After the main device has recovered, the videos recorded on the sub device during the failure period can be transferred to the main device.

Prerequisites

The main device works normally.

Procedure

Step 1 Select **SETTING** > **Cluster Service** > **Transfer Recorder**.

Step 2 Click **Add Task**.

Step 3 Configure parameters.

Step 4 Click **OK**.

You can click to view details on the transferring task.

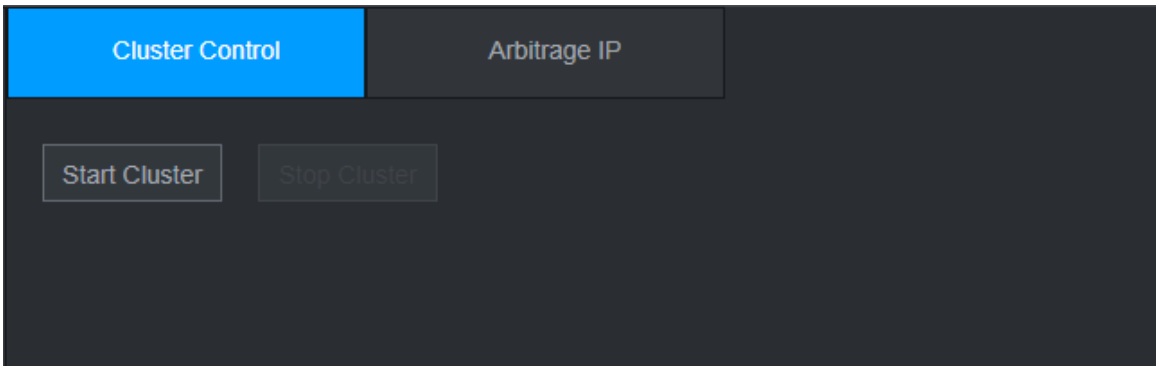
6.4.5 Configuring Cluster Control

6.4.5.1 Cluster Control

Background Information

From **SETTING** > **Cluster Service** > **Cluster Control**, you can enable or disable cluster.

Figure 6-4 Start cluster



You can see the corresponding prompt if you successfully enabled cluster service.

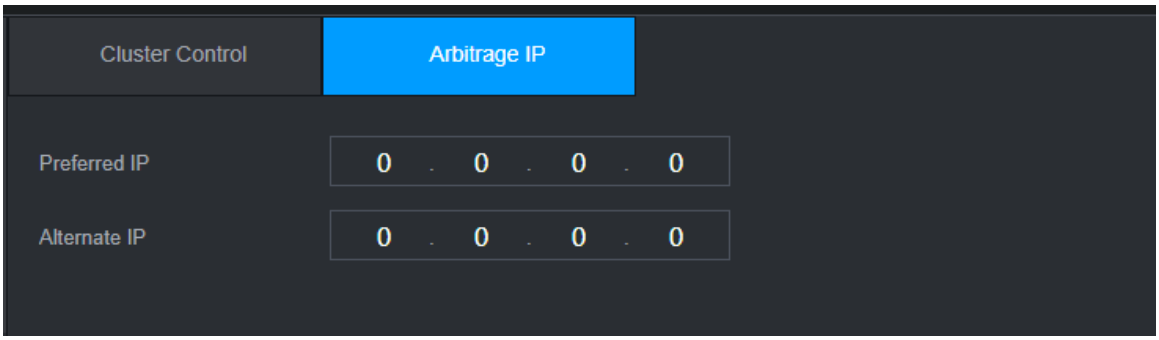
6.4.5.2 Arbitrage IP

When there are only 2 devices in the cluster, a third-party device is required to determine whether the main device is faulty, so arbitration IP must be set for the cluster to perform a normal replacement operation. The arbitration IP can be the IP address of another device, computer or gateway.

Procedure

Step 1 Select **SETTING** > **Cluster Service** > **Arbitrage IP**.

Figure 6-5 Arbitrage IP



Step 2 Configure the preferred and alternate IP.

Step 3 Click **OK**.

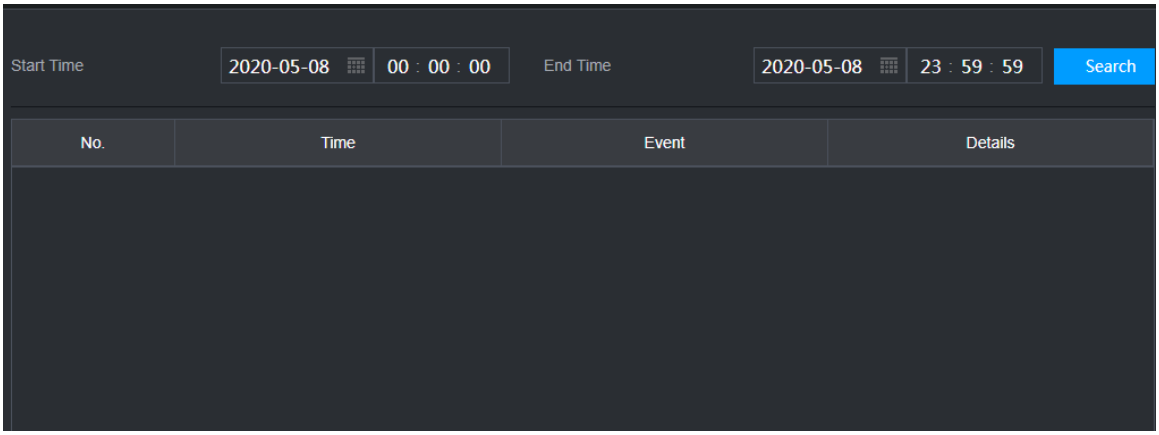
6.4.6 Cluster Log

You can search for and view cluster logs.

Procedure

Step 1 Select **SETTING** > **Cluster Service** > **Cluster Log**.

Figure 6-6 Cluster log



Step 2 Enter the start time and end time.

Step 3 Click **Search**.

7 Glossary

- **DHCP**: DHCP (Dynamic Host Configuration Protocol) is one of the TCP/IP protocol cluster. It is mainly used to assign temporary IP addresses to computers on a network.
- **DDNS**: DDNS (Dynamic Domain Name Server) is a service that maps Internet domain names to IP addresses. This service is useful to anyone who wants to operate a server (web server, mail server, ftp server and more.) connected to the internet with a dynamic IP or to someone who wants to connect to an office computer or server from a remote location with software.
- **eSATA**: eSATA (External Serial AT) is an page that provides fast data transfer for external storage devices. It is the extension specifications of a SATA page.
- **GPS**: GPS (Global Positioning System) is a satellite system, protected by the US, safely orbiting thousands of kilometers above the earth.
- **PPPoE**: PPPoE (Point to Point Protocol over Ethernet) is a specification for connecting multiple computer users on an Ethernet local area network to a remote site. Now the popular mode is ADSL and it adopts PPPoE protocol.
- **Wi-Fi**: Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. The standard is for wireless local area networks (WLANs). It is like a common language that all the devices use to communicate to each other. It is actually IEEE802.11, a family of standard The IEEE (Institute of Electrical and Electronics Engineers Inc.)
- **3G**: 3G is the wireless network standard. It is called 3G because it is the third generation of cellular telecom standards. 3G is a faster network for phone and data transmission and speed Is over several hundred kbps. Now there are four standards: CDMA2000, WCDMA, TD-SCDMA and WiMAX.
- **Dual-stream**: The dual-stream technology adopts high-rate bit stream for local HD storage such as QCIF/CIF/2CIF/DCIF/4CIF encode and one low-rate bit stream for network transmission such as QCIF/CIF encode. It can balance the local storage and remote network transmission. The dual-stream can meet the difference band width requirements of the local transmission and the remote transmission. In this way, the local transmission using high-bit stream can achieve HD storage and the network transmission adopting low bit stream suitable for the fluency requirements of the 3G network such as WCDMA, EVDO, TD-SCDMA.
- **On-off value**: It is the non-consecutive signal sampling and output. It includes remote sampling and remote output. It has two statuses: 1/0.

8 FAQ

Questions	Reasons
The Device failed to start properly.	• Incorrect input power. • Incorrect connection of the power cord. • Damaged power switch. • Wrong program. • Damaged HDD. • Damaged mainboard.
The Device automatically shuts down or stops running.	• Unstable or insufficient input voltage. • Insufficient button power. • Improper operating environment. • Hardware error.
The Device cannot detect HDD.	• Damaged HDD or HDD ribbon. • Loose connection of HDD cable. • Damaged SATA port.
There is no video output in all channels.	• Program version is not correct. • Brightness is 0. • Hardware error.
I cannot find local records.	• Damaged HDD or HDD ribbon. • Program version is not correct. • The recorded file has been overwritten. • The recording function has been disabled.
Distorted recorded videos.	• Video quality setup is too low. • Program read error, bit data is too small. There is mosaic in the full screen. Restart the NVR to solve this problem. • HDD data ribbon error. • HDD malfunction. • NVR hardware malfunctions.
Time display is not correct.	• Setup is not correct. • Battery contact is not correct or voltage is too low. • Crystal is broken.

Questions	Reasons
NVR cannot control PTZ.	• Front panel PTZ error. • PTZ decoder setup, connection or installation is not correct. • Cable connection is not correct. • PTZ setup is not correct. • PTZ decoder and NVR protocol is not compatible. • PTZ decoder and NVR address is not compatible. • When there are several decoders, add 120 Ohm between the PTZ decoder A/B cables furthest end to delete the reverberation or impedance matching. Otherwise the PTZ control is not stable. • The distance is too far.
I cannot log in client-end or web.	• For Windows 98 or Windows ME user, update your system to Windows 2000 sp4. Or you can install client-end software of lower version. Please note right now, our NVR is not compatible with Windows VISTA control. • ActiveX control has been disabled. • No dx8.1 or higher. Upgrade display card driver. • Network connection error. • Network setup error. • Password or username is invalid. • Client-end is not compatible with NVR program.
There is only mosaic no video when preview or playback video file remotely.	• Network fluency is not good. • Client-end resources are limit. • Current user has no right to monitor.
Network connection is not stable.	• Network is not stable. • IP address conflict. • MAC address conflict. • PC or device network card is not good.
Burn error /USB back error.	• Burner and NVR are in the same data cable. • System uses too much CPU resources. Stop record first and then begin backup. • Data amount exceeds backup device capacity. It might result in burner error. • Backup device is not compatible. • Backup device is damaged.
Keyboard cannot control NVR.	• NVR serial port setup is not correct. • Address is not correct. • When there are several switchers, power supply is not enough. • Transmission distance is too far.

Questions	Reasons
Alarm signal cannot be disarmed.	• Alarm setup is not correct. • Alarm output has been open manually. • Input device error or connection is not correct. • Some program versions might have this problem. Upgrade your system.
Alarm function is null.	• Alarm setup is not correct. • Alarm cable connection is not correct. • Alarm input signal is not correct. • There are two loops connect to one alarm device.
Record storage period is not enough.	• Camera quality is too low. Lens is dirty. Camera is installed against the light. Camera aperture setup is not correct. • HDD capacity is not enough. • HDD is damaged.
Cannot playback the downloaded file.	• There is no media player. • No DXB8.1 or higher graphic acceleration software. • There is no DivX503Bundle.exe control when you play the file transformed to AVI via media player. • No DivX503Bundle.exe or ffdshow-2004 1012 .exe in Windows XP OS.
Forgot local menu operation password or network password	Contact your local service engineer or our sales person for help. We can guide you to solve this problem.
There is no video. The screen is in black.	• IPC IP address is not right. • IPC port number is not right. • IPC account (username/password) is not right. • IPC is offline.
The displayed video is not full in the monitor.	Check current resolution setup. If the current setup is 1920*1080, then you need to set the monitor resolution as 1920*1080.
There is no HDMI output.	• Displayer is not in HDMI mode. • HDMI cable connection is not right.
The video is not fluent when I view in multiple-channel mode from the client-end.	• The network bandwidth is not sufficient. The multiple-channel monitor operation needs at least 100M or higher. • Your PC resources are not sufficient. For 16-ch remote monitor operation, the PC shall have the following environment: Quad Core, 2G or higher memory, independent displayer, display card memory 256M or higher.

Questions	Reasons
I cannot connect to the IPC	• Make sure that the IPC has booted up. • IPC network connection is right and it is online • IPC IP is in the blocklist. • The device has connected to the too many IPC. It cannot transmit the video. • Check the IPC port value and the time zone is the same as the NVR. • Make sure current network environment is stable.
After I set the NVR resolution as 1080P, my monitor cannot display.	Shut down the device and then reboot. When you reboot, press the Fn button at the same time and then release after 5 seconds. You can restore NVR resolution to the default setup.
My admin account has been changed and I cannot log in.	Use telnet and then input the following command: cd /mnt/mtd/Config/ rm -rf group rm -rf password Reboot the device to restore the default password.
After I login the Web, I cannot find the remote page to add the IPC.	Clear the Web controls and load again.
There is IP and gateway, I can access the internet via the router. But I cannot access the internet after I reboot the NVR.	Use command PING to check you can connect to the gateway or not. Use telnet to access and then use command "ifconfig –a" to check device IP address. If you see the subnet mask and the gateway has changed after the reboot. Upgrade the applications and set again.
I use the VGA monitor. I want to know if I use the multiple-window mode, I see the video from the main stream or the sub stream?	• For 32-channel series product, the 9/16-window is using the sub stream. • For 4/8/16 series product, system is using the main stream no matter you are in what display mode.

Daily Maintenance

- Use the brush to clean the board, socket connector and the chassis regularly.
- The device shall be soundly earthed in case there is audio/video disturbance. Keep the device away from the static voltage or induced voltage.
- Unplug the power cable before you remove the audio/video signal cable, RS-232 or RS-485 cable.
- Do not connect the TV to the local video output port (VOUT). It might result in video output circuit.
- Always shut down the device properly. Use the shutdown function in the menu, or you can press the power button in the rear pane for at least three seconds to shut down the device. Otherwise it might result in HDD malfunction.
- Make sure the device is away from the direct sunlight or other heating sources. Keep the sound ventilation.
- Check and maintain the device regularly.

Appendix 1 HDD Capacity Calculation

Calculate the total capacity needed by each device according to video recording (video recording type and video file storage time).

1. According to Formula (1) to calculate storage capacity q_i that is the capacity of each channel needed for each hour, unit Mbyte.

$$q_i = d_i \div 8 \times 3600 \div 1024 \quad (1)$$

In the formula: d_i means the bit rate, unit Kbit/s

2. After video time requirement is confirmed, according to Formula (2) to calculate the storage capacity m_i, which is storage of each channel needed unit Mbyte.

$$m_i = q_i \times h_i \times D_i \quad (2)$$

In the formula:

h_i means the recording time for each day (hour)

D_i means number of days for which the video shall be kept

3. According to Formula (3) to calculate total capacity (accumulation) q_T that is needed for all channels in the device during **scheduled video recording**.

$$q_T = \sum_{i=1}^{c} m_i \quad (3)$$

In the formula:

c means total number of channels in one device

4. According to Formula (4) to calculate total capacity (accumulation) q_T that is needed for all channels in device during **alarm video recording (including motion detection)**.

$$q_T = \sum_{i=1}^{c} m_i \times a\% \quad (4)$$

In the formula: $a\%$ means alarm occurrence rate

Appendix 2 Mouse Operation

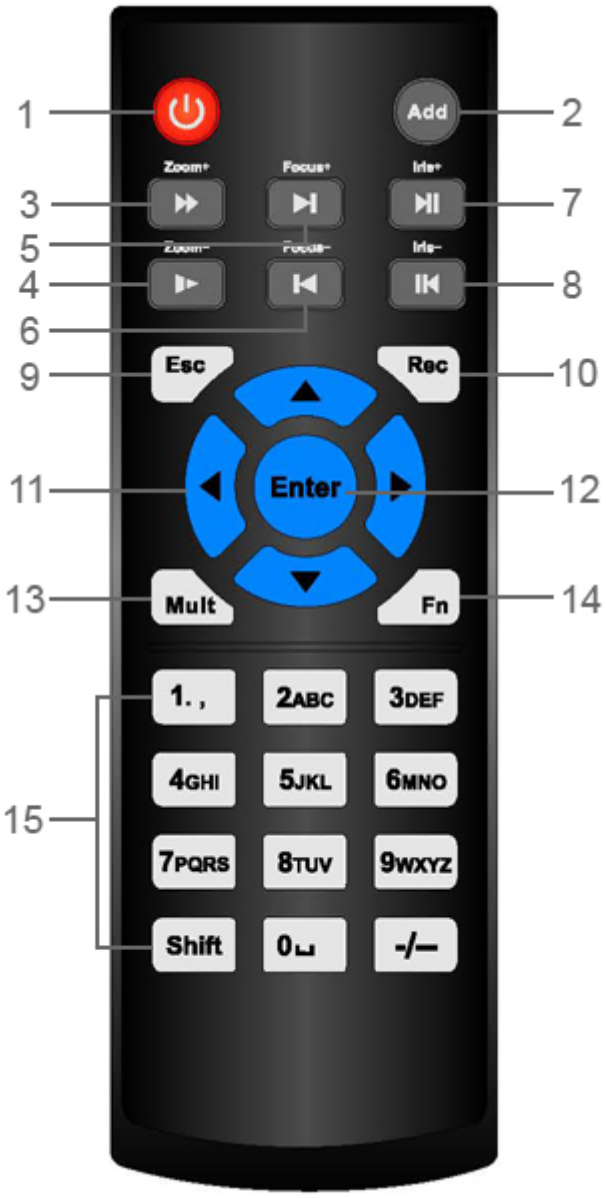
Appendix Table 2-1Mouse operation

Operation	Description
Left click mouse	When you have selected one menu item, left click mouse to view menu content.
	Modify checkbox or motion detection status.
	Click combo box to pop up drop-down list
	In input box, you can select input methods. Left click the corresponding button on the panel you can input numeral/English character (lower case/ upper case). Here ← stands for backspace button. __ stands for space button. In English input mode: _ stands for input a backspace icon and ← stands for deleting the previous character. In numeral input mode: _ stands for clear and ← stands for deleting the previous numeral.
Double left click mouse	Implement special control operation such as double click one item in the file list to playback the video.
	In multiple-window mode, double left click one channel to view in full-window. Double left click current video again to go back to previous multiple-window mode.
Right click mouse	In real-time monitor mode, pops up shortcut menu.
	Exit current menu without saving the modification.
Press middle button	In numeral input box: Increase or decrease numeral value.
	Switch the items in the checkbox.
	Page up or page down.
Move mouse	Select current control or move control.
Drag mouse	Select motion detection zone.
	Select privacy mask zone.

Appendix 3 Remote Control

Remote control is not our standard accessory and it is not included in the accessory package.

Appendix Figure 3-5 Remote control



No.	Name	Function
1	Power button	Press this button to boot up or shut down the device.
2	Address	Press this button to input device serial number, so that you can control the Device.
3	Forward	Multi-step forward speed and normal speed playback.
4	Slow motion	Multi-step slow motion speed or normal playback.
5	Next record	In playback state, press this button to play back the next video.

No.	Name	Function
6	Previous record	In playback state, press this button to play back the previous video.
7	Play/Pause	• In normal playback state, press this button to pause playback. • In pause state, press this button to resume to normal playback. • In live view window page, press this button to enter video search menu.
8	Reverse/pause	In the reverse playback state, press this button to pause reverse playback.
		In the reverse playback pause state, press this button to resume to playback reversing state.
9	Esc	Go back to previous menu or cancel current operation (close front page or control).
10	Record	• Start or stop record manually. • In record page, use the direction buttons to select the channel that you want to record. • Press this button for at least 1.5 seconds, and the manual record page will be displayed.
11	Direction keys	Switch between current activated controls by going left or right. In playback state, the keys control the playback progress bar. Aux function (such as operating the PTZ menu).
12	Enter/menu key	• Confirms an operation. • Go to the OK button. • Go to the menu.
13	Multiple-window switch	Switch between multiple-window and one-window.
14	Fn	• In single-channel monitoring mode, press this button to display the PTZ control and color setting functions. • Switch the PTZ control menu in PTZ control page. • In motion detection page, press this button with direction keys to complete setup. • In text mode, press and hold this button to delete the last character. To use the clearing function: Long press this button for 1.5 seconds. • In HDD menu, switch HDD recording time and other information as indicated in the pop-up message.
15	Alphanumeric keys	• Input password, numbers. • Switch channel. • Press Shift to switch the input method.

Appendix 4 Compatible Network Camera List

Please note all the models in the following list for reference only. For those products not included in the list, please contact your local retailer or technical supporting engineer for detailed information.

Appendix Table 4-2Compatible network camera list

Manufacturer	Model	Version	Video Encode	Audio/ Video	Protocol
AXIS	P1346	5.40.9.2	H264	√	ONVIF/Private
	P3344/ P3344-E	5.40.9.2	H264	√	ONVIF/Private
	P5512	—	H264	√	ONVIF/Private
	Q1604	5.40.3.2	H264	√	ONVIF/Private
	Q1604-E	5.40.9	H264	√	ONVIF/Private
	Q6034E	—	H264	√	ONVIF/Private
	Q6035	5.40.9	H264	√	ONVIF/Private
	Q1755	—	H264	√	ONVIF/Private
	M7001	—	H264	√	Private
	M3204	5.40.9.2	H264	√	Private
	P3367	HEAD LFP4_0 130220	H264	√	ONVIF
	P5532-P	HEAD LFP4_0 130220	H264	√	ONVIF
ACTi	ACM-3511	A1D-220-V3.12.15-AC	MPEG4	√	Private
	ACM-8221	A1D-220-V3.13.16-AC	MPEG4	√	Private
Arecont	AV1115	65246	H264	√	Private
	AV10005DN	65197	H264	√	Private
	AV2115DN	65246	H264	√	Private
	AV2515DN	65199	H264	√	Private
	AV2815	65197	H264	√	Private
	AV5115DN	65246	H264	√	Private
	AV8185DN	65197	H264	√	Private
Bosch	NBN-921-P	—	H264	√	ONVIF
	NBC-455-12P	—	H264	√	ONVIF
	VG5-825	9500453	H264	√	ONVIF
	NBN-832	66500500	H264	√	ONVIF
	VEZ-211-IWTEIVA	—	H264	√	ONVIF

Manufacturer	Model	Version	Video Encode	Audio/ Video	Protocol
	NBC-255-P	15500152	H264	√	ONVIF
	VIP-X1XF	—	H264	√	ONVIF
Brikcom	B0100	—	H264	√	ONVIF
	D100	—	H264	√	ONVIF
	GE-100-CB	—	H264	√	ONVIF
	FB-100A	v1.0.3.9	H264	√	ONVIF
	FD-100A	v1.0.3.3	H264	√	ONVIF
Cannon	VB-M400	—	H264	√	Private
CNB	MPix2.0DIR	XNETM1120111229	H264	√	ONVIF
	VIPBL1.3MIRVF	XNETM2100111229	H264	√	ONVIF
	IGC-2050F	XNETM2100111229	H264	√	ONVIF
CP PLUS	CP-NC9-K	6.E.2.7776	H264	√	ONVIF/Private
	CP-NC9W-K	6.E.2.7776	H264	√	Private
	CP-ND10-R	cp20111129ANS	H264	√	ONVIF
	CP-ND20-R	cp20111129ANS	H264	√	ONVIF
	CP-NS12W-CR	cp20110808NS	H264	√	ONVIF
	VS201	cp20111129NS	H264	√	ONVIF
	CP-NB20-R	cp20110808BNS	H264	√	ONVIF
	CP-NT20VL3-R	cp20110808BNS	H264	√	ONVIF
	CP-NS36W-AR	cp20110808NS	H264	√	ONVIF
	CP-ND20VL2-R	cp20110808BNS	H264	√	ONVIF
	CP-RNP-1820	cp20120821NSA	H264	√	Private
	CP-RNC-TP20FL3C	cp20120821NSA	H264	√	Private
	CP-RNP-12D	cp20120828ANS	H264	√	Private
	CP-RNC-DV10	cp20120821NSA	H264	√	Private

Manufacturer	Model	Version	Video Encode	Audio/ Video	Protocol
	CP-RNC-DP20FL2C	cp20120821NSA	H264	√	Private
Dynacolor	ICS-13	d20120214NS	H264	√	ONVIF/Private
	ICS-20W	vt20111123NSA	H264	√	ONVIF/Private
	NA222	—	H264	√	ONVIF
	MPC-IPVD-0313	k20111208ANS	H264	√	ONVIF/Private
	MPC-IPVD-0313AF	k20111208BNS	H264	√	ONVIF/Private
Honeywell	HIDC-1100PT	h.2.2.1824	H264	√	ONVIF
	HIDC-1100P	h.2.2.1824	H264	√	ONVIF
	HIDC-0100P	h.2.2.1824	H264	√	ONVIF
	HIDC-1300V	2.0.0.21	H264	√	ONVIF
	HICC-1300W	2.0.1.7	H264	√	ONVIF
	HICC-2300	2.0.0.21	H264	√	ONVIF
	HDZ20HDX	H20130114NSA	H264	√	ONVIF
LG	LW342-FP	—	H264	√	Private
	LNB5100	—	H264	√	ONVIF
Imatek	KNC-B5000	—	H264	√	Private
	KNC-B5162	—	H264	√	Private
	KNC-B2161	—	H264	√	Private
Panasonic	NP240/CH	—	MPEG4	√	Private
	WV-NP502	—	MPEG4	√	Private
	WV-SP102H	1.41	H264	√	ONVIF/Private
	WV-SP105H	—	H264	√	ONVIF/Private
	WV-SP302H	1.41	H264, MPEG4	√	ONVIF/Private
	WV-SP306H	1.4	H264, MPEG4	√	ONVIF/Private
	WV-SP508H	—	H264, MPEG4	√	ONVIF/Private
	WV-SP509H	—	H264, MPEG4	√	ONVIF/Private
	WV-SF332H	1.41	H264, MPEG4	√	ONVIF/Private

Manufacturer	Model	Version	Video Encode	Audio/ Video	Protocol
	WV-SW316H	1.41	H264, MPEG4	√	ONVIF/Private
	WV-SW355H	1.41	H264, MPEG4	√	ONVIF/Private
	WV-SW352H	—	H264, MPEG4	√	ONVIF/Private
	WV-SW152E	1.03	H264, MPEG4	√	ONVIF/Private
	WV-SW558H	—	H264, MPEG4	√	ONVIF/Private
	WV-SW559H	—	H264, MPEG4	√	ONVIF/Private
	WV-SP105H	1.03	H264, MPEG4	√	ONVIF/Private
	WV-SW155E	1.03	H264, MPEG4	√	ONVIF/Private
	WV-SF336H	1.44	H264, MPEG4	√	ONVIF/Private
	WV-SF332H	1.41	H264, MPEG4	√	ONVIF/Private
	WV-SF132E	1.03	H264, MPEG4	√	ONVIF/Private
	WV-SF135E	1.03	H264, MPEG4	√	ONVIF/Private
	WV-SF346H	1.41	H264, MPEG4	√	ONVIF/Private
	WV-SF342H	1.41	H264, MPEG4	√	ONVIF/Private
	WV-SC385H	1.08	H264, MPEG4	√	ONVIF/Private
	WV-SC386H	1.08	H264, MPEG4	√	ONVIF/Private
	WV-SP539	1.66	H264, MPEG4	√	ONVIF
	DG-SC385	1.66	H264, MPEG4	√	ONVIF
PELCO	IXSOLW	1.8.1-20110912-1.9082-A1.6617	H264	√	Private
	IDE20DN	1.7.41.9111-O3.6725	H264	√	Private

Manufacturer	Model	Version	Video Encode	Audio/ Video	Protocol
	D5118	1.7.8.9310-A1.5288	H264	√	Private
	IM10C10	1.6.13.9261-O2.4657	H264	√	Private
	DD4N-X	01.02.0015	MPEG4	√	Private
	DD423-X	01.02.0006	MPEG4	√	Private
	D5220	1.8.3-FC2-20120614-1.9320-A1.8035	H264	√	Private
Samsung	SNB-3000P	2.41	H264, MPEG4	√	ONVIF/Private
	SNP-3120	1.22_110120_1	H264, MPEG4	√	ONVIF/Private
	SNP-3370	1.21_110318	MPEG4	√	Private
	SNB-5000	2.10_111227	H264, MPEG4	√	ONVIF/Private
	SND-5080	—	H264, MPEG4	√	Private
	SNZ-5200	1.02_110512	H264, MPEG4	√	ONVIF/Private
	SNP-5200	1.04_110825	H264, MPEG4	√	ONVIF/Private
	SNB-7000	1.10_110819	H264	√	ONVIF/Private
	SNB-6004	V1.0.0	H264	√	ONVIF
Sony	SNC-D H110	1.50.00	H264	√	ONVIF/Private
	SNC-CH120	1.50.00	H264	√	ONVIF/Private
	SNC-CH135	1.73.01	H264	√	ONVIF/Private
	SNC-CH140	1.50.00	H264	√	ONVIF/Private
	SNC-CH210	1.73.00	H264	√	ONVIF/Private
	SNC-D H210	1.73.00	H264	√	ONVIF/Private
	SNC-D H240	1.50.00	H264	√	ONVIF/Private
	SNC-D H240-T	1.73.01	H264	√	ONVIF/Private
	SNC-CH260	1.74.01	H264	√	ONVIF/Private
	SNC-CH280	1.73.01	H264	√	ONVIF/Private
	SNC-RH-124	1.73.00	H264	√	ONVIF/Private
	SNC-RS46P	1.73.00	H264	√	ONVIF/Private
	SNC-ER550	1.74.01	H264	√	ONVIF/Private

Manufacturer	Model	Version	Video Encode	Audio/ Video	Protocol
	SNC-ER580	1.74.01	H264	√	ONVIF/Private
	SNC-ER580	1.78.00	H264	√	ONVIF
	SNC-VM631	1.4.0	H264	√	ONVIF
	WV-SP306	1.61.00	H264, MPEG4	√	SDK
	WV-SP306	1.61.00	H264	√	ONVIF
	SNC-VB600	1.5.0	H264	√	Private
	SNC-VM600	1.5.0	H264	√	Private
	SNC-VB630	1.5.0	H264	√	Private
	SNC-VM630	1.5.0	H264	√	Private
SANYO	VCC-HDN4000PC	—	H264	√	ONVIF

Appendix 5 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations from Dahua on how to create a more secured security system.

Mandatory actions to be taken for basic device network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

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

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

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

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

1. **Physical Protection**

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

2. **Change Passwords Regularly**

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

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

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

4. **Enable Account Lock**

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

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

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

6. **Enable HTTPS**

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

7. **MAC Address Binding**

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

8. **Assign Accounts and Privileges Reasonably**

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

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

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

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

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

10. **Audio and Video Encrypted Transmission**

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

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

11. **Secure Auditing**

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

12. **Network Log**

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

13. **Construct a Safe Network Environment**

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

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

More information

Please visit Dahua official website security emergency response center for security announcements and the latest security recommendations.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No. 1399, Binxing Road, Binjiang District, Hangzhou, P. R. China | Website: www.dahuasecurity.com | Postcode: 310053
Email: dhoverseas@dhvisiontech.com | Tel: +86-571-87688888 28933188