



Milesight OpenVision Server User Manual

Applicable Model: SE0216R-K, SE0232R-K

Version: 1.0

Date: 2026-09-11

Table of contents

Chapter 1. Introduction	3
1.1 Copyright Statement	3
1.2 Safety and Regulatory Information	3
1.3 Revision History	4
Chapter 2. Product Description	4
2.1 Product Overview	5
2.2 Key Specifications	5
2.3 Hardware Overview	7
2.4 Related Documents	9
Chapter 3. Configuration Flow	10
Chapter 4. Installation	11
Chapter 5. Device Access	14
5.1 Powering on the Device	14
5.2 Assigning an IP Address	14
5.2.1 Assigning an IP Address s Using Smart Tools	14
5.2.2 Assigning an IP Address s via Browser	16
Chapter 6. Web Settings	18
6.1 Overview	18
6.1.1 Key Features	18
6.1.2 Login	19
6.2 Media	19
6.2.1 Audio	19
6.3 Network	21
6.3.1 Basic	21
6.4 Storage	28
6.4.1 Storage Management (for SE0216R)	28
6.4.2 Storage Management (for SE0232R)	30
6.5 Event	35
6.5.1 Basic Event	35
6.6 VMS Edge	39
6.6.1 Server	40
6.6.2 File Manager	42
6.6.3 Smart Tools Lite	44
6.7 System	49
6.7.1 System Setting	49
6.7.2 Security	51
6.7.3 Logs	57
6.7.4 Maintenance	58
Chapter 7. Integration with Nx Witness Server	60
Chapter 8. FAQ	70
Chapter 9. Services	73

Chapter 1. Introduction

1.1 Copyright Statement

This manual may not be reproduced in any form or by any means to create any derivative such as translation, transformation, or adaptation without the prior written permission of Milesight IoT Co., Ltd (Hereinafter referred to as Milesight).



reserves the right to change this manual and the specifications without prior notice. The latest specifications and user documentation for all Milesight products are available on our official website <https://www.milesight.com/security/>.

1.2 Safety and Regulatory Information

1.2.1 Safety Instructions

Read these safety instructions carefully before installing, operating, or servicing the product.

- Use only the power adapter supplied with the product or a power adapter approved by the manufacturer.
- The power supply used with this product shall provide the specified 12 V DC output and sufficient rated output current.
- Do not use a damaged power adapter, power cord, or DC power cable.
- Disconnect the power supply before installing, removing, opening, or servicing the equipment.
- Do not block the ventilation openings. Ensure adequate airflow around the equipment.
- Keep the equipment away from water, excessive moisture, heat sources, and direct sunlight.
- This product is intended for indoor use only.
- Operate the product only within the operating temperature and humidity ranges specified in this manual.

Power Supply

- Device Input: 12 V DC
- Rated Current: 6.6 A
- Rated Power: 80 W

Use only the supplied or manufacturer-approved AC/DC power adapter that meets the electrical ratings specified for this product.

Using an incompatible power adapter may result in equipment damage, overheating, fire, or other safety hazards.

1.2.2 FCC Compliance Information

(1) FCC Part 15 Compliance Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference

2. This device must accept any interference received, including interference that may cause undesired operation.

(2) Class A Digital Device Notice

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

1.2.3 EU Conformity Statement

This product complies with the following directives and standards:

- CE Marking: This product conforms to the essential requirements of the EU Directive 2014/30/EU (EMC), 2014/35/EU (LVD), and 2011/65/EU (RoHS).
- FCC Statement: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.
- RoHS: This product complies with EU RoHS Directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment.
- RCM Statement: This product complies with the applicable requirements of the Australian and New Zealand Regulatory Compliance Mark (RCM), including electrical safety and electromagnetic compatibility (EMC) regulations.
- WEEE Directive 2012/19/EU: Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.

1.3 Revision History

Table 1. Revision History

Version	Software Version	System Version	Revision Content	Release Date
V1.0	OV_81.8.0.5-r1-NX	OVSsystem 81.8.0.4-r1	First Release	September 2026

Chapter 2. Product Description

2.1 Product Overview

Milesight OpenVision Server offers a pre-configured, plug-and-play surveillance platform with the Nx Witness Server seamlessly embedded. Designed for fast and hassle-free deployment, it combines powerful hardware and intelligent video management software in one compact system. With its user-friendly design and robust performance, the Milesight OpenVision Server is ideal for outdoor edge deployment scenarios, providing a streamlined, cost-effective, and smart security solution.

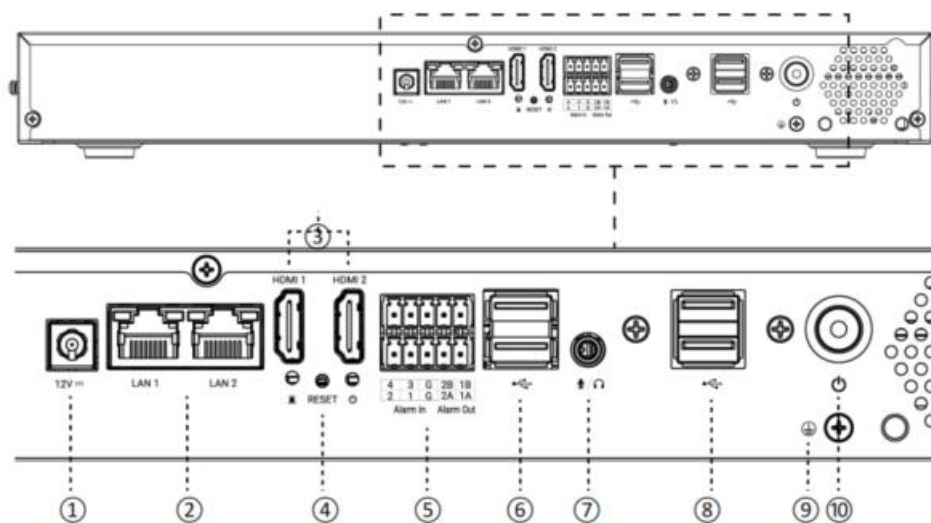
2.2 Key Specifications

	Model	SE0216R	SE0232R
System	Main Processor	Intel Quad Core @3.40 GHz Max	
	Memory	4GB LPDDR5	8GB LPDDR5
	Firmware Storage	32GB eMMC	
	Operating System	Linux Ubuntu 24.04 LTS	
	GPU Options	Integrated GPU	
	TPM	fTPM	
	System Compatibility	API, ONVIF, Network Optix API	
	System Language	English, Traditional Chinese, French, Spanish, Italian, Japanese, Dutch, German, Polish, Ukrainian, Swedish, Danish, Icelandic, Norwegian, Finnish	
Storage	HDD	2 × SATA ports, up to 24TB per disk, max 48TB total	
	RAID	NA	RAID1 (2* HDD)
	SSD	2* SATA SSD, 1* M.2 M-Key NVMe SSD	
	NAS	NAS mounting via web (NFS/SMB protocols)	
	File Manager	Web-based file management (upload/download/move)	
	Storage Mode	Continuous, Motion, Objects, Events, Dual Stream	
Audio	Compression	G.711/AAC/G.722/G.726	
	Audio Communication	2-way	
	Audio Broadcast	ONVIF-based Audio Broadcast	
Event	Basic Event	Audio Alarm, Network Disconnected, IP Address Conflict, SSD/HDD Full, SSD/HDD Uninitialized, SSD/HDD Error, No SSD/HDD, Low Voltage, ONVIF Alarm Input	Audio Alarm, Network Disconnected, IP Address Conflict, SSD/HDD/RAID Full, SSD/HDD/RAID Uninitialized, SSD/HDD/RAID Error, No SSD/HDD/RAID, Low Voltage, ONVIF Alarm Input
	Alarm Action	Event-triggered audio alarm, ONVIF alarm output control, etc	
Application	NX Witness Server	Support (include Plug-in)	
	ONVIF Device	Support	

Management	Web Management	Support (network, audio, storage, event, system configuration, etc.)	
	Web File Manager	Support	
	Smart Tool Lite	Built-in Smart Tool Lite: Supports camera search, IP editing, activation, etc.	
	Maintenance	Firmware Upgrade, Auto Reboot, Scheduled Reboot, Factory Reset, etc.	
Performance	Video Inputs	Max. 16CH	Max. 32CH
	Video Resolution	12MP ~ CIF	
	Network Bandwidth	Max. 144 Mbps recording, Max. 144 Mbps outgoing	Max. 288 Mbps recording, Max. 288 Mbps outgoing
	Metadata Performance	64 targets/s (AI by Camera)	128 targets/s (AI by Camera, store the database on the SSD) 42 targets/s (AI by Camera, store the database on the HDD)
	Video Compression	H.265, H.264, MJPEG	
	Decoding Capability	NX Server: Support Hardware Decoding	
	Edge Analytics	Analytics Events (Based on camera metadata): CCTV (Intrusion Detection / Region Entrance / Region Exit / Advanced Motion Detection / Line Crossing / Loitering / Object Left / Object Removed / Object Counting / Regional People Counting); LPR (Attribute Event / Black List / White List / Visitor Event / Speed Monitoring / No Plates / Reverse Driving); Object Detected Events (person and vehicle with attribute / face)	
		Smart Search (Based on camera metadata): CCTV: Person (Hat, Top Clothing Color, Bottom Clothing Color), Vehicle (Vehicle Type), Face (Gender, Age, Mask, Cap, Glasses); LPR: Vehicle (Color, Vehicle Type, Brand, Speed, Direction), License Plate (Number, Color, Country, Plate Type)	
Network	Protocol	IPv4, IPv6, TCP/IP, UDP/IP, RTP (UDP), RTP (TCP), RTSP, NTP, HTTP, DHCP (Client), ICMP, IGMP, ARP, DNS, HTTPS, ONVIF, NFS, SMB	
Interface	Ethernet	2* 2500Mbps RJ45 Ethernet Port	
	Link Aggregation	Active Backup, Link Aggregation Control Protocol (LACP), and Balance-RR	
	HDMI Output	2 × HDMI Port (For Testing, CLI Output Only) HDMI1&2: 3840x2160/60Hz, 1920x1080/60Hz. Simultaneous mode (simultaneously outputs video sources for HDMI1-2 ports).	
	Audio	1x 3.5mm Headphone Jack with Microphone Input (4-pole, TRRS, CTIA Standard)	

General	Alarm I/O	4 Alarm input / 2 Alarm Output
	Back Panel Indicator Light	2 (Power & Alarm Light)
	Front Panel Indicator Light	3 (System & Storage & Power)
	Power Button	Yes
	Reset Button	Yes
	USB Interface	4* USB 3.0, 1* USB 2.0
	Power Supply	12V (Built-in 100-240V AC 80W power adapter)
	Consumption	Typical: 9W (Without HDD/SSD, DC), MAX: 39W (With 2* HDD, DC)
	Working Temperature	-10°C to 55°C
	Working Humidity	10% to 90% RH (no freezing and no condensation)
	Cooling System	Fan cooling
	Product Dimension	380mm(W) x 317.6mm(D) x 51.8mm(H)
	Installation	19-inch rack mounting or desktop placement
	Net Weight (Without HDD)	2.7 Kg
	Package Weight	4 Kg
	Warranty	3 Years

2.3 Hardware Overview



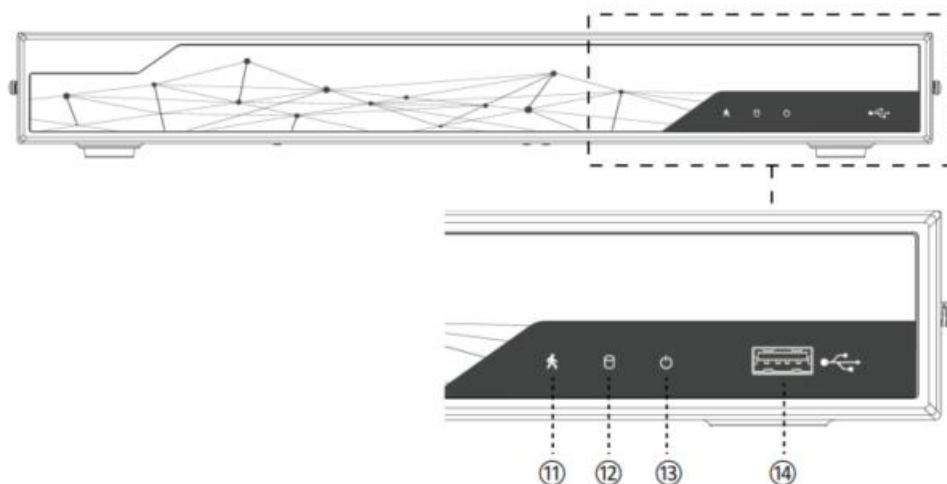
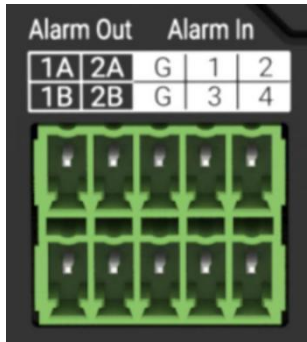


Table 2. Interfaces Description

No.	Interfaces	Key Specifications	Function & Usage
1	Power Supply	DC 12V±15% (5525 DC power plug)	Connects the external power adapter to supply power.
2	Ethernet Port	2* 2500Mbps RJ45 Ethernet Port, Lan1 support POE PD	Supports network connectivity and PoE+ power receiving via Ethernet cable.
3	HDMI Port	2	For testing and CLI output only; no local video output
4	Reset Button	1	(1) Factory Reset: Hold the Reset button before powering on, continue holding until the status LED flashes 10 times and turns solid. This restores factory defaults and clears all data. (2) Configuration Reset: Press and hold Reset for 10 seconds while the device is running. This restores configuration settings while retaining the IP address and user information.
5	Alarm I/O	4*Alarm Input: Wet Contact (5V) or Dry Contact / 2*Alarm Output: Dry Contact (Rated Voltage 24V / Current 1A)	Used to connect external devices, such as speakers, or alarm systems.  • Alarm In 1/2/3/4: Used to connect different alarm input devices. Each port is functionally identical and is numbered for easy device

			identification. • G (GND): Ground terminal for alarm input devices. Connect here together with Alarm In to complete the circuit. • 1A, 1B / 2A, 2B: Used for alarm output. Each pair (e.g., 1A and 1B) forms a relay output circuit for external alarm output devices (such as warning lights).
6	USB Interface	2* USB 3.0	Used to connect various external devices such as a mouse and keyboard, enabling data transmission and device control.
7	Audio	1* 3.5mm Headphone Jack with Microphone Input (4- pole, TRRS, CTIA Standard)	Supports two-way audio via headset with microphone.
8	USB Interface	2* USB 3.0	Used to connect various external devices such as a mouse and keyboard, enabling data transmission and device control.
9	Grounding Hole	1	Connects a grounding wire to prevent static damage.
10	Power Button	1	Press this button to power on the device.
11	Run LED	1	✓ Blinks once per second (green): Server is operating normally ✓ Blinks five times per second (green): Firmware is upgrading ✓ Off: Indicator turns off during upgrade reboot
12	HDD LED	1	✓ Solid green: HDD or SSD detected and available ✓ Blinks once per second (green): HDD/SSD is being accessed ✓ Fast blinking (green, five times per second): At least one disk has failed, but others are running normally ✓ Off: No available HDD/SSD, or all disks have failed
13	Power LED	1	✓ System is starting up (boot in progress) ✓ Blinking green (1 flash per second): System startup complete, running normally
14	USB Interface	1* USB 2.0	Used to connect various external devices such as a mouse and keyboard, enabling data transmission and device control.

2.4 Related Documents

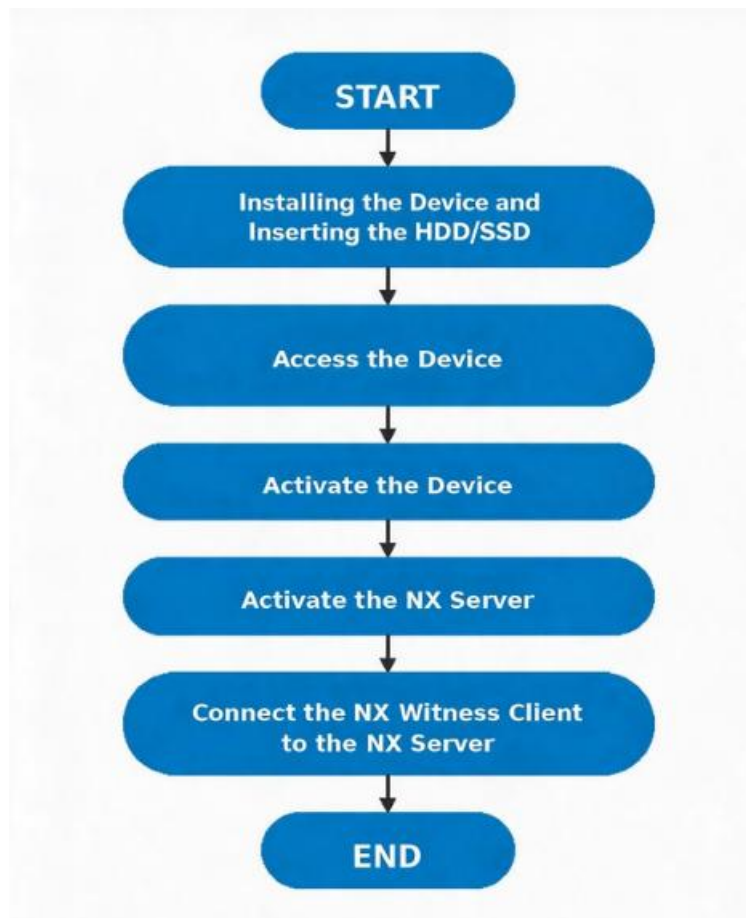
Table 3. Related Documents

Document Type	Link
Datasheet	16CH: https://drive.google.com/file/d/1q4JnlUzf-DHL-0uzaDu0y13aAlaegads/view?usp=drive_link

	32CH: https://drive.google.com/file/d/1ltmz7H4u5sKs36KfMwhPDG5dz-I9Pt7T/view?usp=drive_link
Quick Start Guide	https://drive.google.com/file/d/1zBmQT6OdQJTG0tMY5SRlr64uJphVhpgW/view?usp=drive_link

Chapter 3. Configuration Flow

The configuration flow of Milesight OpenVision Server is shown in the following figure.



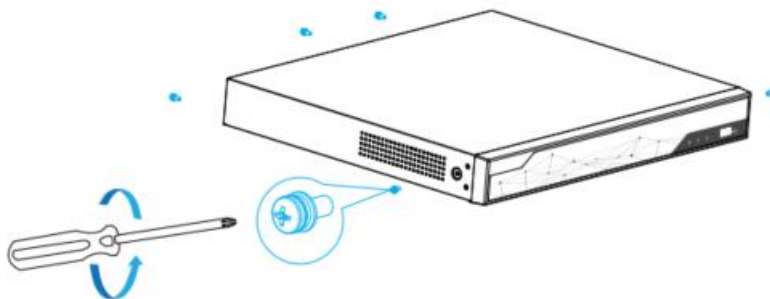
More configuration details are shown in the following table.

Table 4. Description of flow

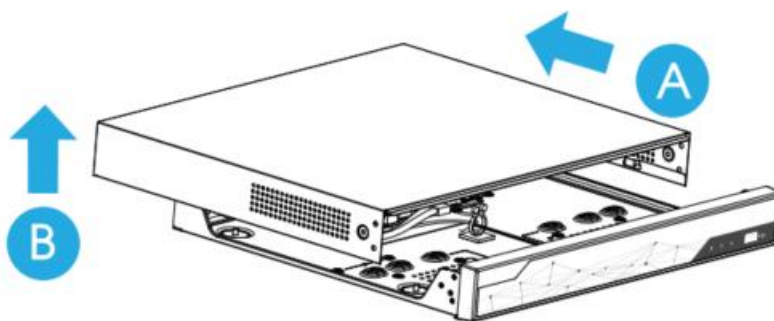
Configuration	Reference
Installation	Chapter 4. Installation
Access the Device	Chapter 5. Device Access
Activate the Device	5.2 Assigning an IP Address
Activate the Nx Witness Server	6.5.2 Server

Chapter 4. Installation

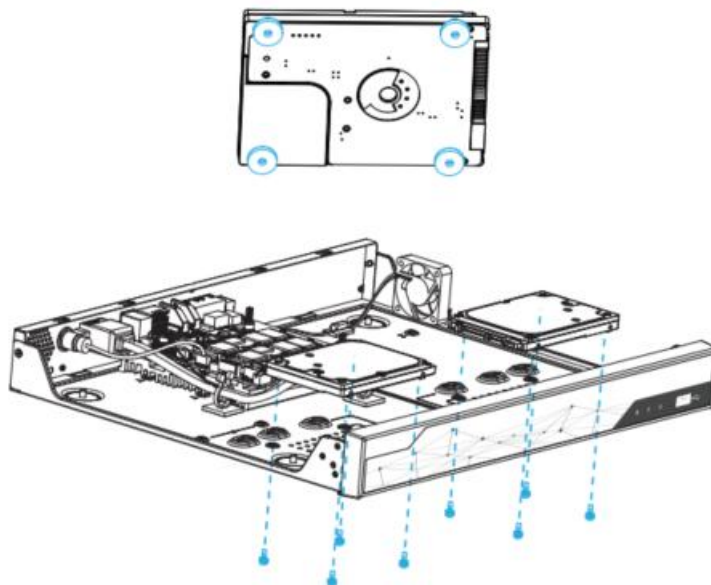
Step 1: Using a cross screwdriver to remove the screws at the rear panel and side panel in an anticlockwise direction.



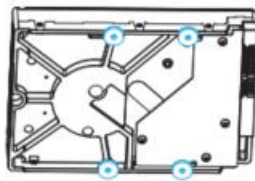
Step 2: Slide the upper casing to the rear first and lift it up.



Step 3: Vibration damping pads MUST be applied to HDD mounting holes

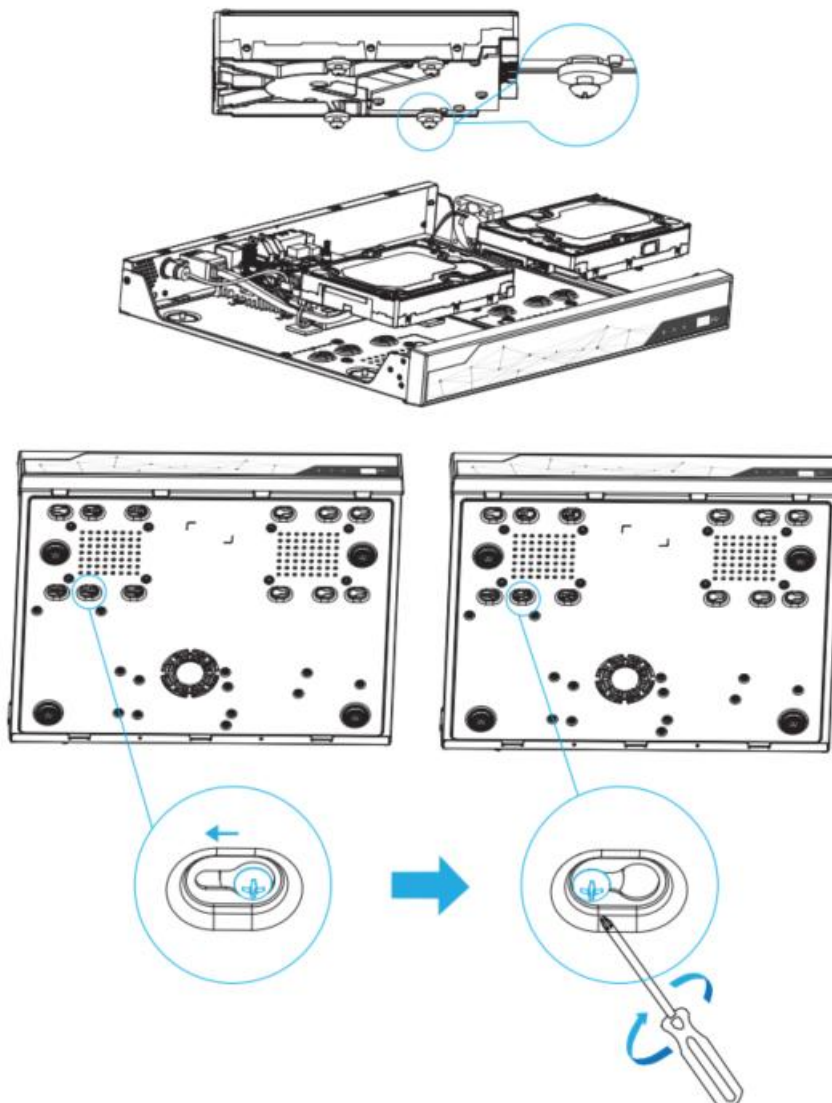


2.5-inch Hard Drive Installation Steps

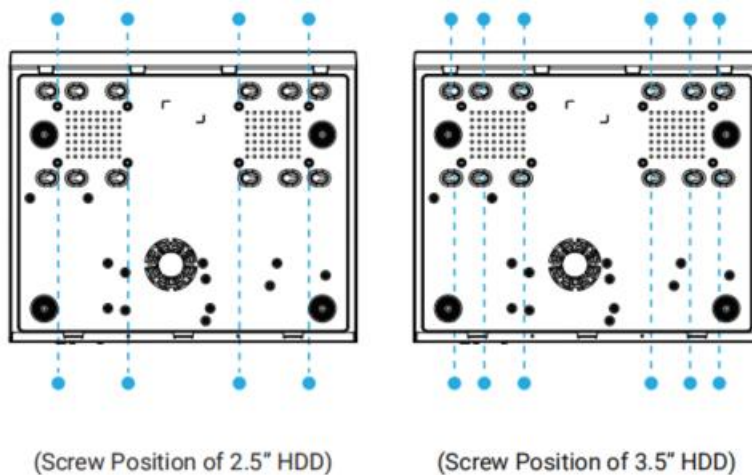


3.5-inch Hard Drive Installation

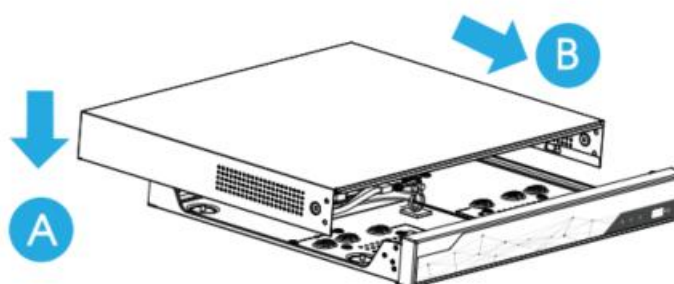
Pre-tighten screws — do NOT fully tighten



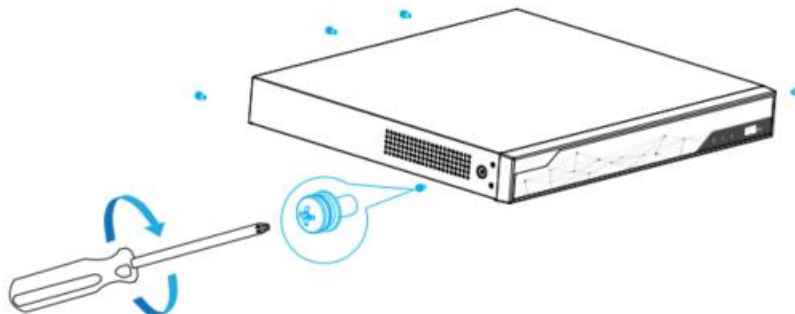
Step 4: After that, check if all the screws are tightened. Then connect the power cable and data cable to each HDD.



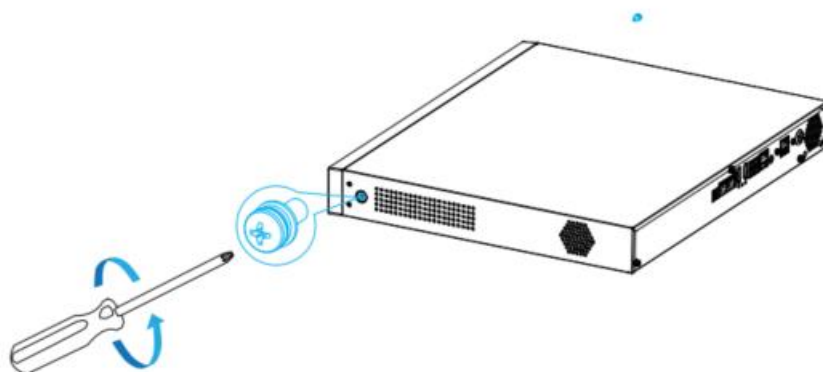
Step5: Pull down the upper casing and slide it to the front.

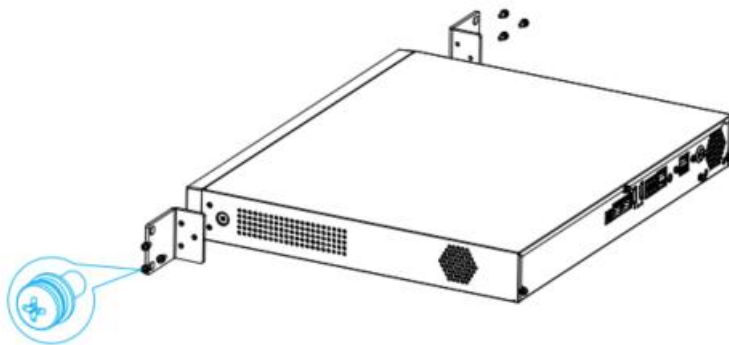


Step6: Lock the screws on the rear panel and side panel.



Step7: Install the ear mounts for rack-mounting in standard cabinets. Remove the two pre-installed screws on each side panel, then secure the ear mount brackets to both sides using three screws each.





Chapter 5. Device Access

5.1 Powering on the Device

Install the HDD/SSD and power on the device.

Note: If you do not have an HDD/SSD and want to test the system first, please refer to the "Test Mode (No HDD/SSD)" section below.

5.2 Assigning an IP Address

The product must be assigned an IP address to be accessible.

Default Network Configuration:

LAN 1: DHCP is enabled by default. If DHCP address acquisition fails (e.g., no DHCP server available), the device falls back to the factory default static IP 192.168.5.190.

LAN 2: Static IP 192.168.6.190 (default).

Note: If both LAN ports are configured with IP addresses in the same subnet, a routing conflict will occur. The system will automatically disable one interface to avoid network issues. Please ensure LAN 1 and LAN 2 use different network segments.

You can discover and change the IP address of the device via Smart Tools (recommended) or a web browser. Please ensure your computer is connected to the same physical network as the device.

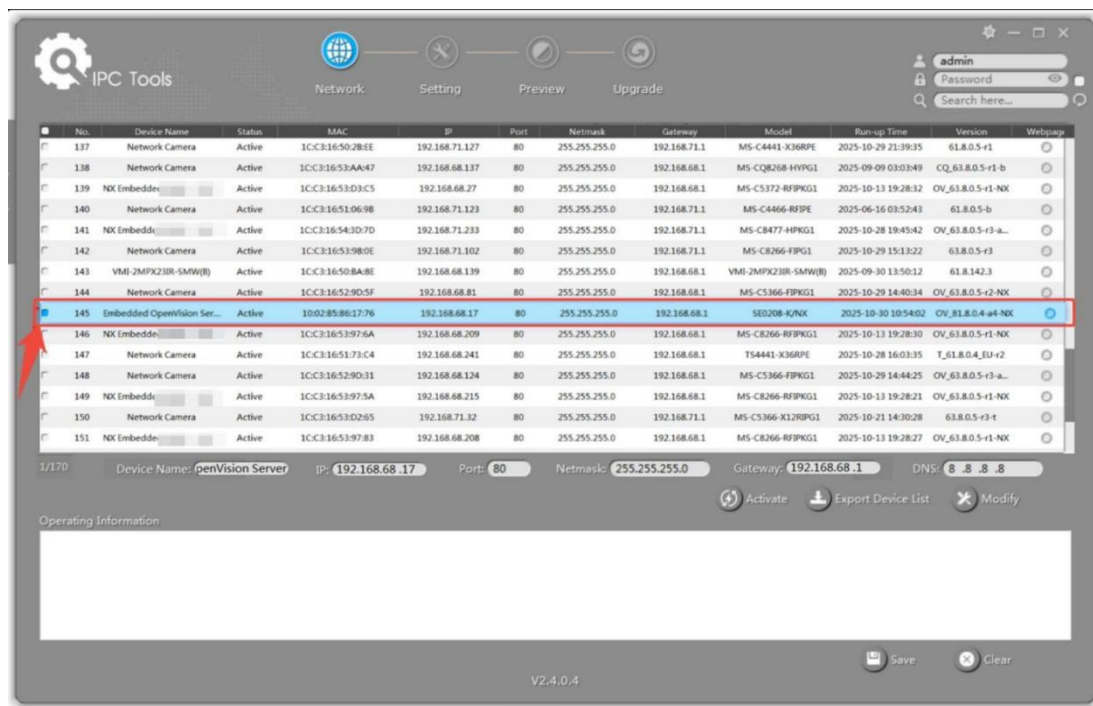
5.2.1 Assigning an IP Address Using Smart Tools

Smart Tools is a software tool which can automatically detect multiple online Milesight network cameras and devices in the LAN, set IP addresses, and manage firmware upgrades. It's recommended to use when assigning IP addresses for multiple cameras.

Step 1: Install Smart Tools (The software could be downloaded from our website: [Milesight Auxiliary Software](#));

Step 2: Start Smart Tools, click the IPC Tools page, then enter the device information, such as IP address, MAC address, Status, Port number, Netmask, and Gateway, then all related Milesight devices in the same network will be displayed. Details are shown as the figure below;

Step 3: Select the device according to the MAC addresses;

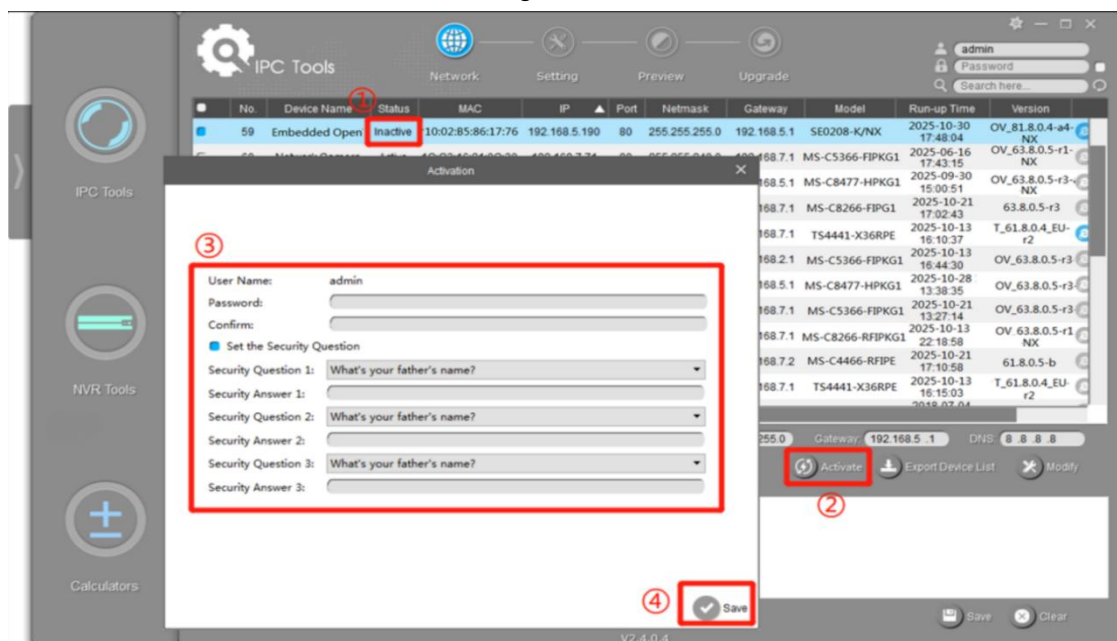


Step 4: If the selected device shows "Inactive" in the status bar, click "Activate" to set the password when using it for the first time. You can also set the security questions when activating the device in case that you forget the password (You can reset the password by answering three security questions correctly). Click 'Save' and it will show that the activation was successful.

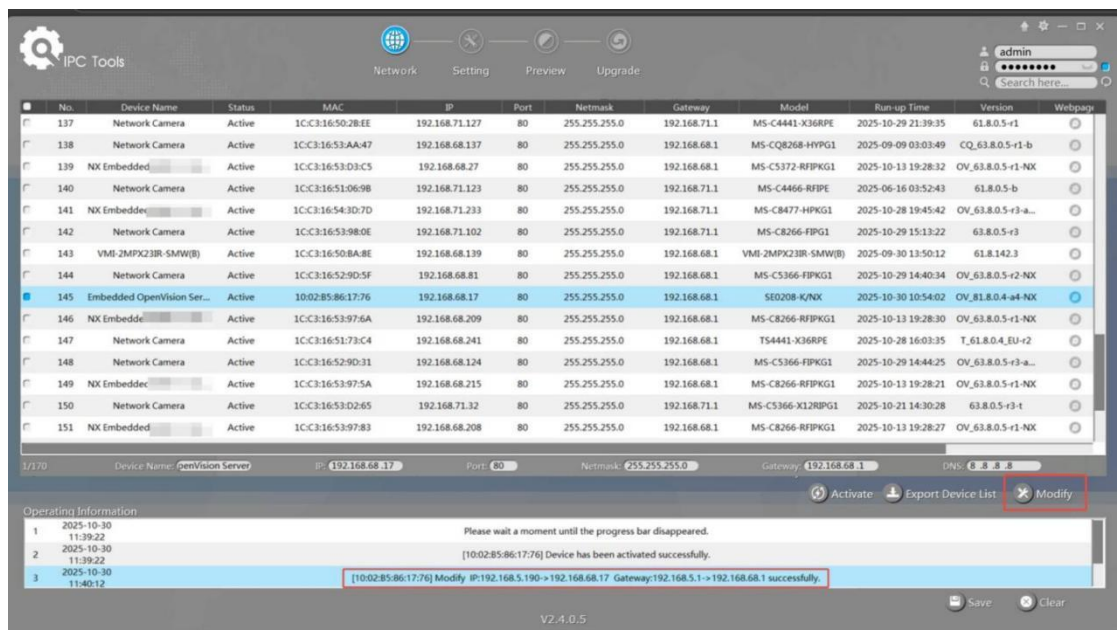


Note:

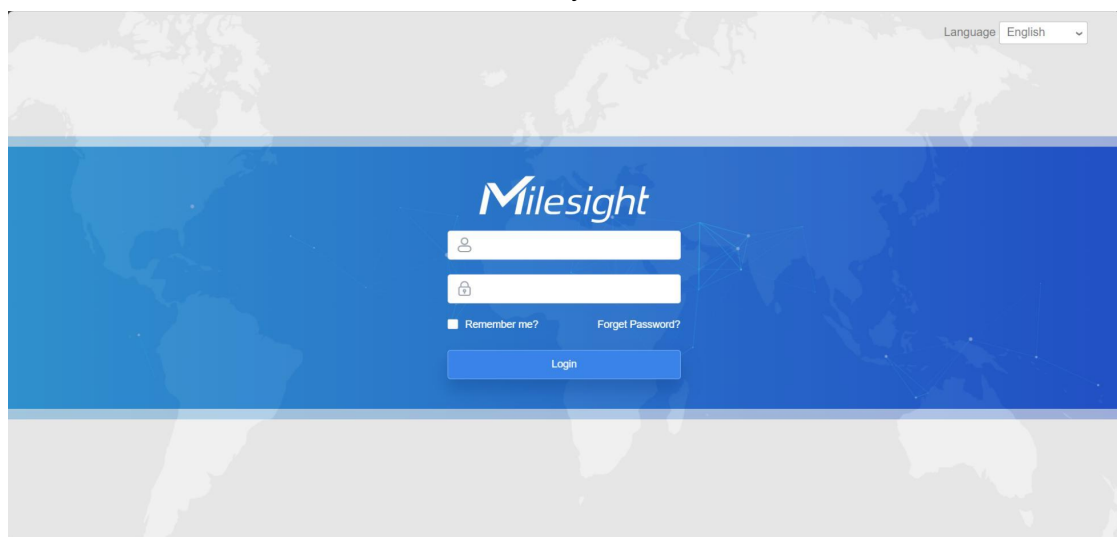
Password must be 8 to 32 characters long, contain at least one number and one letter.



Step 5: After activation, you can change the IP address or other network values, and then click "Modify" button.



Step 6: By double clicking the selected device or the browser of interested device, you can access the device via web browser directly.



More usage of Smart Tools, please refer to the [Smart Tools User Manual](#).

5.2.2 Assigning an IP Address via Browser

Important: Before proceeding, confirm the current IP address of LAN 1:

- If the device obtained an IP via DHCP, use that IP address.
- If DHCP fails (e.g., direct connection to PC without router), the device falls back to the last confirmed static IP address. If no static IP was previously configured, it reverts to the factory default 192.168.5.190.

If you know the device's current IP address and your computer is on the same network segment, you can access the device directly via browser. Otherwise, follow these steps:

Step 1: Change the IP address of your computer to match the device's network segment.

If accessing via DHCP-obtained IP: Ensure your computer is on the same subnet as the DHCP-assigned address (e.g., if device got 192.168.1.x, set your PC to 192.168.1.x).

If accessing via fallback IP 192.168.5.190: Set your computer to the 192.168.5.0 segment.

Two ways to add an IP address on Windows:

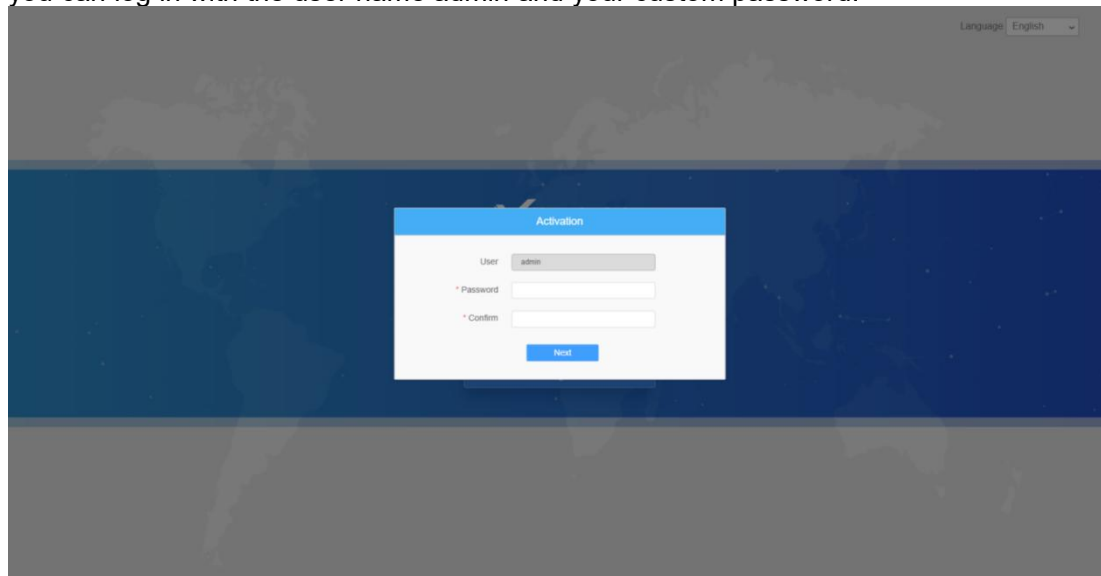
a. Start → Control Panel → Network and Internet Connection → Network Connection → Local Area Connection, and double-click it;

b. Click "Advanced", and then click "IP settings" → "IP address" → "Add". In the pop-up window, enter an IP address in the same segment as the device (e.g., 192.168.5.61, but please ensure this IP address does not conflict with existing network devices);

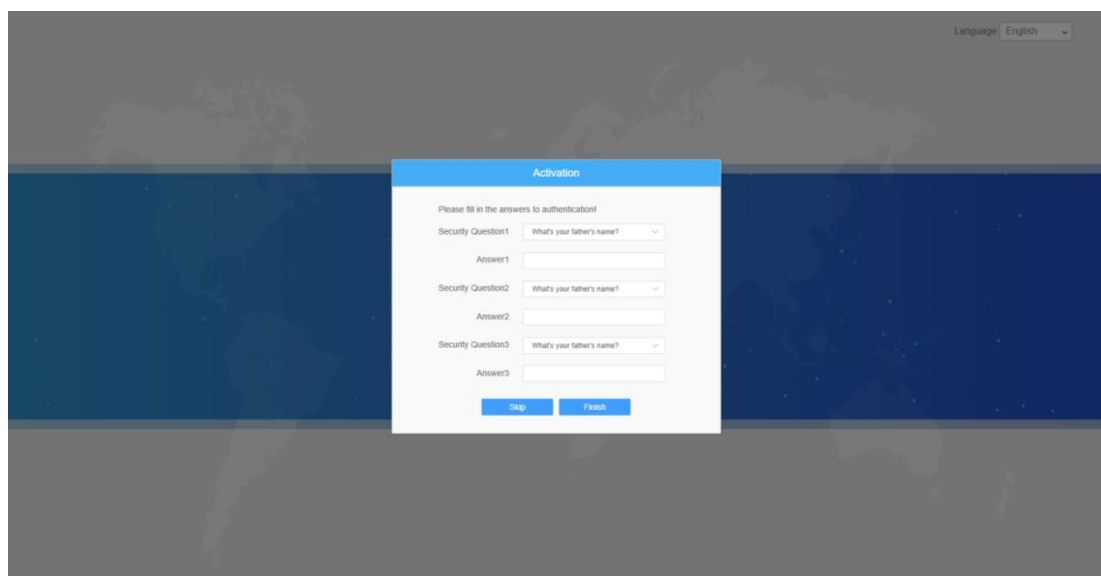
Step 2: Start the browser. In the address bar, enter the device's IP address:

- If DHCP succeeded: `http://<DHCP-assigned-IP>` (check router or use Smart Tools to discover)
- If DHCP failed: `http://192.168.5.190`

Step 3: When using the device for the first time, you need to activate it by setting a password. You can also set three security questions for your device after activation. Then you can log in with the user name admin and your custom password.



The screenshot shows the 'Activation' page of the OpenVision Server. The page has a dark blue header with a 'Language: English' dropdown. The main content area is a light gray rectangle with a blue border. Inside, there's a white box with the title 'Activation'. Below the title, there are three input fields: 'User' (pre-filled with 'admin'), 'Password' (with an asterisk), and 'Confirm' (with an asterisk). A blue 'Next' button is at the bottom of the white box.



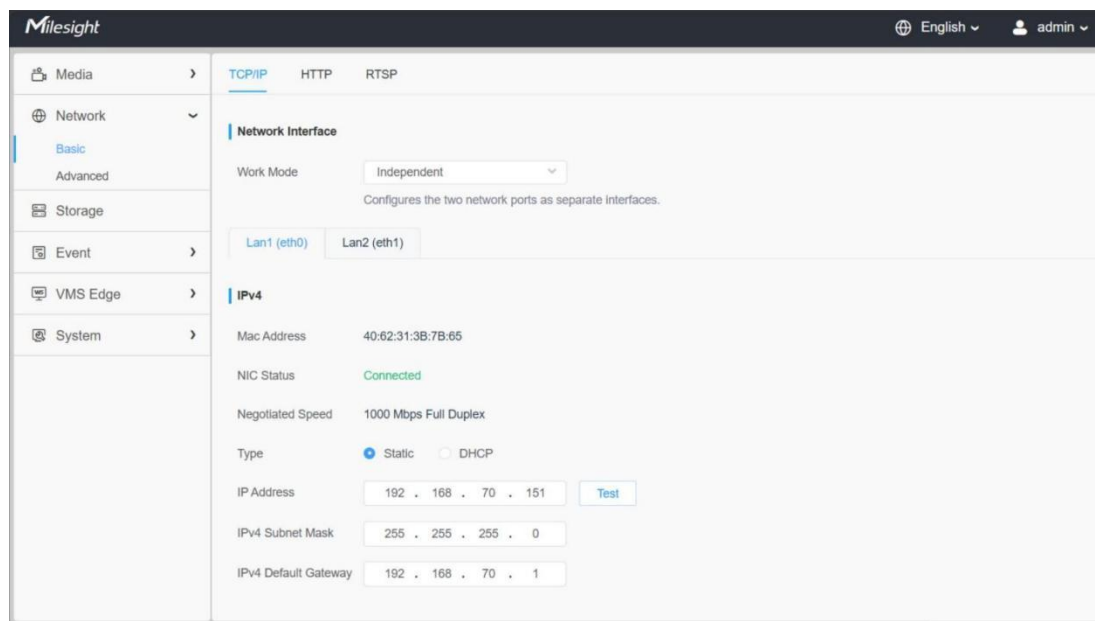
The screenshot shows the 'Activation' page of the OpenVision Server. The page has a dark blue header with a 'Language: English' dropdown. The main content area is a light gray rectangle with a blue border. Inside, there's a white box with the title 'Activation'. Below the title, there's a section titled 'Please fill in the answers to authentication!'. It contains three rows, each with a 'Security Question' dropdown (all pre-filled with 'What's your father's name?') and an 'Answer' input field. At the bottom of the white box, there are two blue buttons: 'Skip' and 'Finish'.



Note:

- Password must be 8 to 32 characters long, contain at least one number and one letter
- You can click the "forget password" in login page to reset the password by answering three security questions when you forget the password, if you set the security questions in advance.

Step 4: After login, please select “Settings” --> “Network” --> “Basic” --> “TCP/IP”. The Network Settings page appears (Shown as below Figure);



Step 5: Change the IP address or other network values. Then click “Save” button;

Step 6: The change of default IP address is completed.

Chapter 6. Web Settings

6.1 Overview

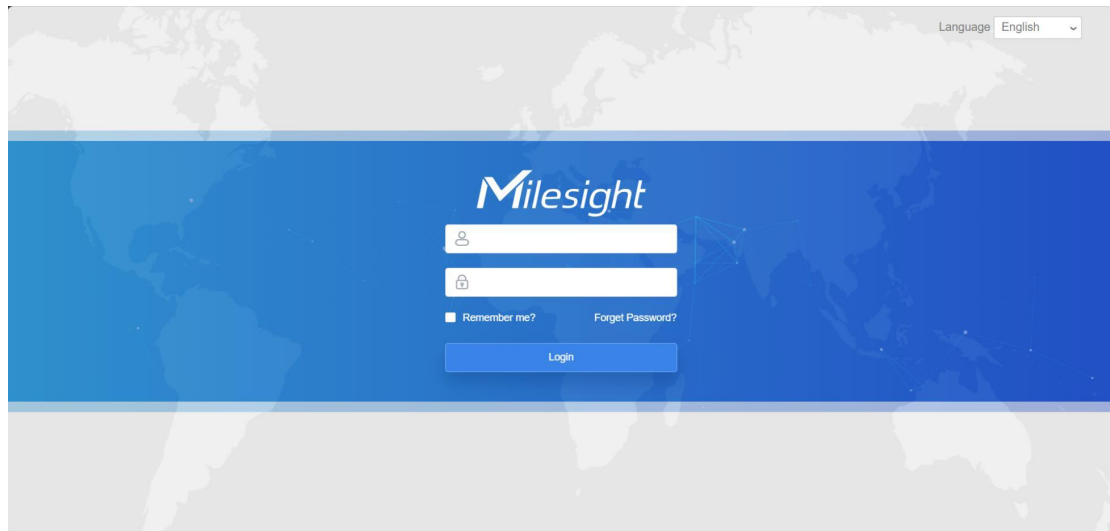
6.1.1 Key Features

Key Features of Web Page

- Supports remote web login (via router port forwarding).
- Supports IP configuration and device information synchronization using the Smart tools.
- Supports link aggregation.
- Supports firmware upgrades.
- Supports basic maintenance functions, such as scheduled reboot and factory reset.
- Supports ONVIF server (can be added to Nx Witness for alarm integration and audio integration).
- Supports linked audio broadcasting.
- Supports storage management, SSD health monitoring and fault alerts, and NAS mounting via the web interface.
- Support RAID 1 for 32-channel OpenVision Server models (HDDs only).
- Supports automatic time synchronization, IP whitelist, and system logs.

- Supports multiple languages.
- Supports Nx Witness Server management tools and configuration optimization.
- Supports Test Mode for temporary server operation without SSD/HDD after unboxing.
- Supports Web File Manager.

6.1.2 Login



Before configuring Milesight OpenVision Server via the web interface, please ensure:

1. The device has been equipped with the HDD/SSD.
2. The device has been activated and assigned a valid IP address.

For detailed activation steps, please refer to [Chapter 5](#).

Once all the above preparations are complete, you can access the web interface by entering the device IP address in your browser, then log in with the username and password you set during activation.

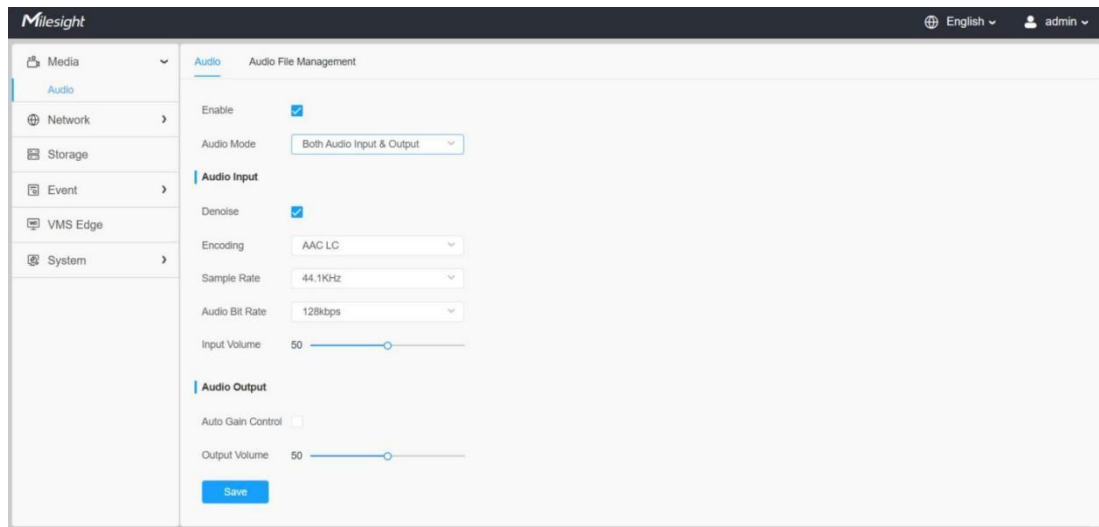
6.2 Media

6.2.1 Audio

6.2.1.1 Audio

This audio function allows to configure the audio interface parameters for the Milesight OpenVision Server.

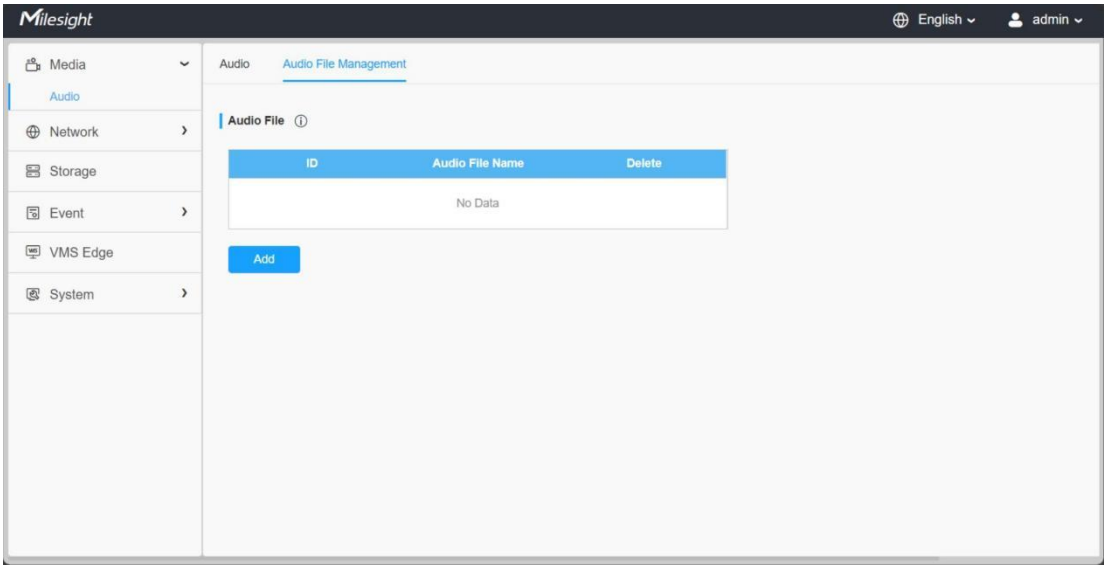
Before configuring it, please ensure that the audio input and output devices are properly connected to the audio port of the product.

**Table 5. Description of the buttons**

Parameters	Function Introduction
Enable	Check on the checkbox to enable audio feature.
Audio Mode	Audio Input/Audio Output/Both Audio Input & Output are optional.
Audio Input	Denoise: Set it as On/Off. When you set the function on, the noise detected can be filtered. Encoding: G.711-ULaw, G.711-ALaw, AAC LC, G.722 and G.726 are available Sample Rate: 8KHz, 16KHz, 32KHz, 44.1KHz, and 48KHz are available. Audio Bit Rate: The function is available only for AAC LC, and supports up to 256kbps. Input Volume: Input audio gain level, 0-100.
Audio Output	Auto Gain Control: Enable this function to improve the quality of audio. Output Volume: Adjust volume of output.

6.2.1.2 Audio File Management

You can upload up to 5 audio files manually on the Audio web page and you can also edit the audio file's name when upload.



Note:
Support audio files with codec type PCM/MP3/AAC, no more than 5MB!

6.3 Network

6.3.1 Basic

6.3.1.1 TCP/IP

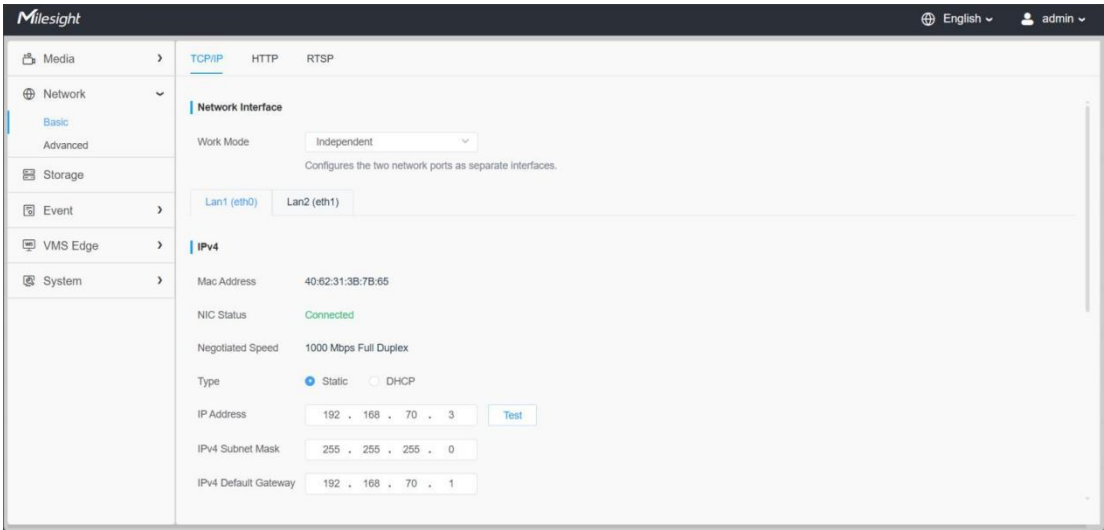
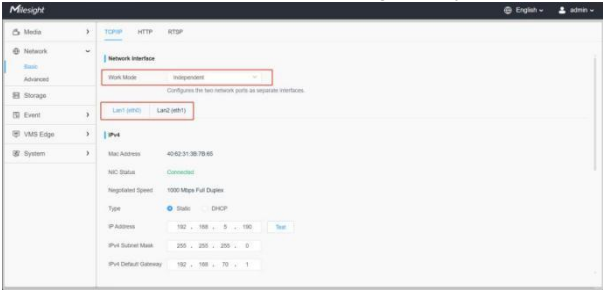
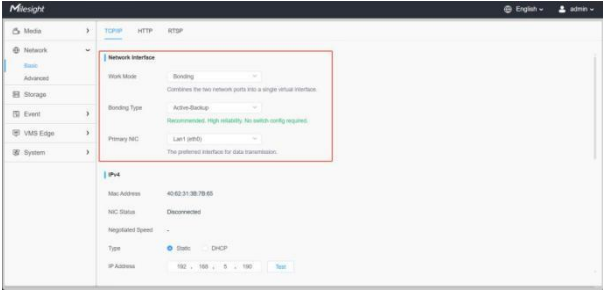
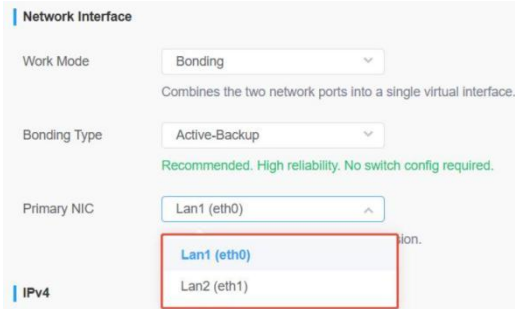


Table 6. Description of the buttons

Parameters	Function Introduction
Network Interface	Work Mode: Here you can select the working mode for the dual network ports. - Independent: The two ports (Lan1, Lan2) work separately. Each port can have its own IP address, subnet mask, gateway, etc.  Note: - Lan1: DHCP is enabled by default. If DHCP fails (e.g., direct connection to PC without router), the device falls back to the last confirmed static IP address. If no static IP was previously configured, it reverts to the factory default 192.168.5.190. - Lan2: Static IP 192.168.6.190 (default). The VMS license is bound to LAN 1 by default. To avoid license disruption, it is strongly recommended to use LAN1 as the priority. - Bonding: The two ports are aggregated into one logical interface for link redundancy or load balancing. Only the bonded virtual interface needs to be configured. Note: In Bonding mode, DHCP is enabled by default on the bond0 interface. If DHCP address acquisition fails (e.g., no DHCP server available), the device falls back to the last confirmed static IP address configured on bond0. If no static IP was previously configured, it reverts to the factory default 192.168.5.190.  • Bonding Type: - Active-Backup: Only one port is active at a time; the other acts as a backup. If the active port fails, the backup takes over. - LACP: Dynamic link aggregation. Both ports work simultaneously, increasing total bandwidth and providing fault tolerance. - Balance-RR: Round-robin load balancing. Both ports work simultaneously, increasing total bandwidth and providing fault tolerance.

	c. Balance-RR: Round-robin load balancing. Packets are transmitted alternately between the two ports, which can increase throughput.
Parameters	Function Introduction
Network Interface	Primary NIC: This option specifies the preferred interface for data transmission.  If the preferred port fails (e.g., cable unplugged, link down), the system automatically switches to the other port to maintain network connectivity.
IPv4	Type: Static Type and DHCP Type are optional for user to get IPv4 address automatically or use fixed IP address. IPv4 Address: An address that used to identify a network device on the network.  Note: The Test button is used to test if the IP is conflicting. IPv4 Subnet Mask: It is used to identify the subnet where the network device is located. IPv4 Default Gateway: The default router address. Preferred DNS Server: The DNS Server translates the domain name to IP address.
IPv6	IPv6 Mode: Choose different modes for IPv6: Manual/Auto(RA/SLAAC)/ DHCPv6 IPv6 Address: IPv6 Address used to identify a network device on the network. IPv6 Prefix: Define the prefix length of IPv6 address. IPv6 Default Gateway: The default router IPv6 address.
MTU	Maximum Transmission Unit. The default value is 1500. You can customize the value from 1200 to 1500 as needed.
	Save the configuration.

6.3.1.2 HTTP

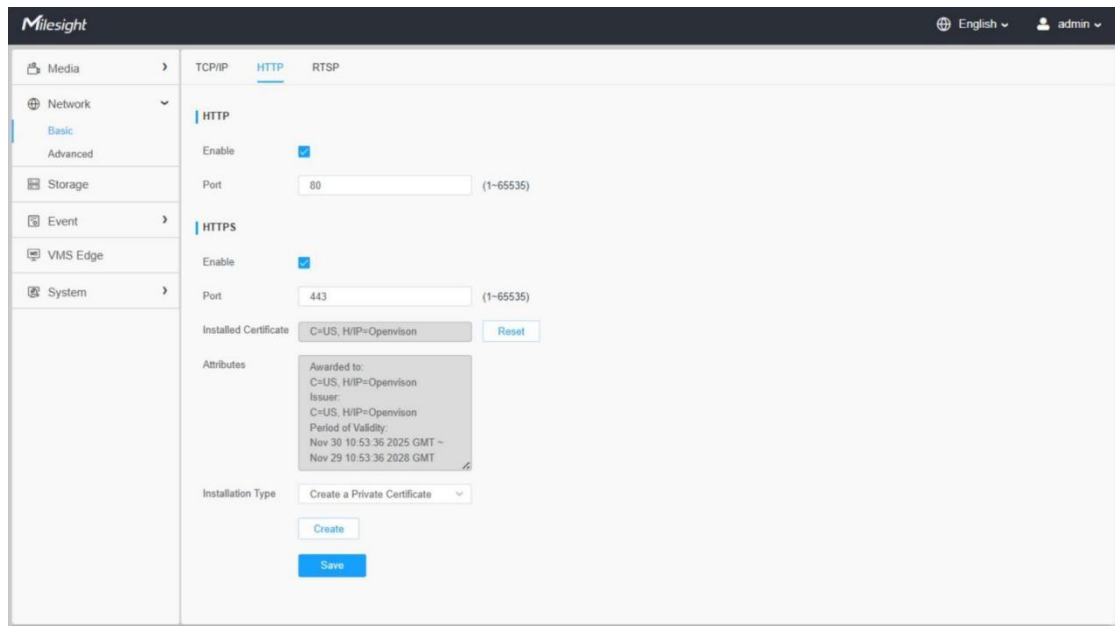


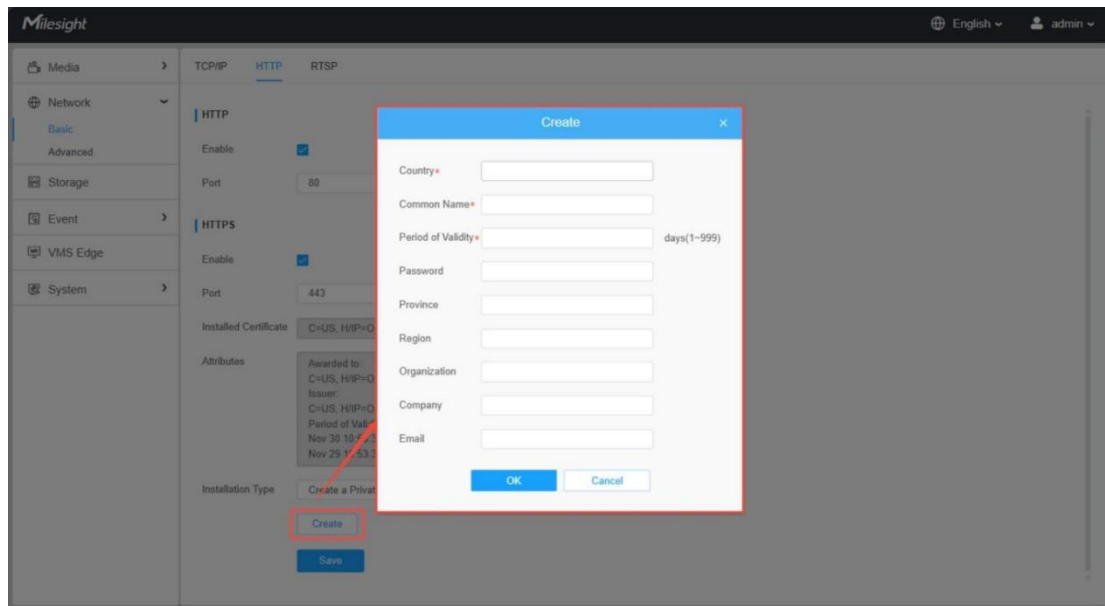
Table 7. Description of the buttons

Parameters	Function Introduction
HTTP	Enable: Start or stop using HTTP. Port: Web GUI login port, the default is 80, the same with ONVIF port.
HTTPS	Enable: Start or stop using HTTPS. Port: Web GUI login port via HTTPS, the default is 443. Note: For more details about how to use enable HTTPS access, please refer to https://milesight.freshdesk.com/a/solutions/articles/69000797384.
Installed Certificate	Upload and set the SSL certificate.
Attributes	
Installation Type	
Save	Save the configuration.

There are three certificate installation types:

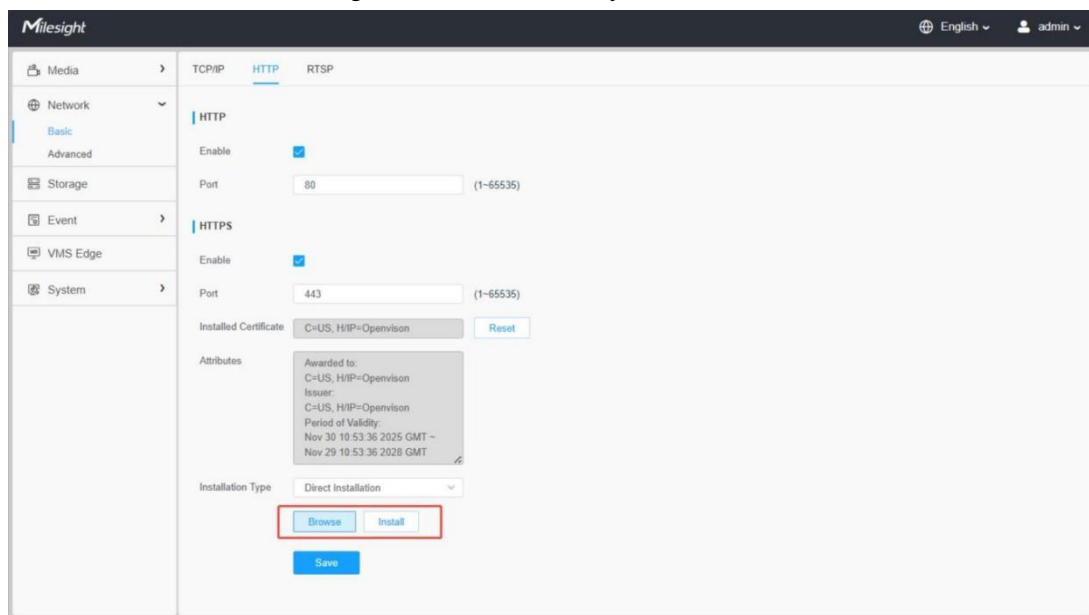
- Create a Private Certificate:

Click “Create” to create the following dialog box. And then enter Country, Common Name, Period of Validity and other information. And then click “OK” to generate a private certificate.



- Direct Installation:

Click “Browse” to select a signed certificate locally and click “Install” to install it.

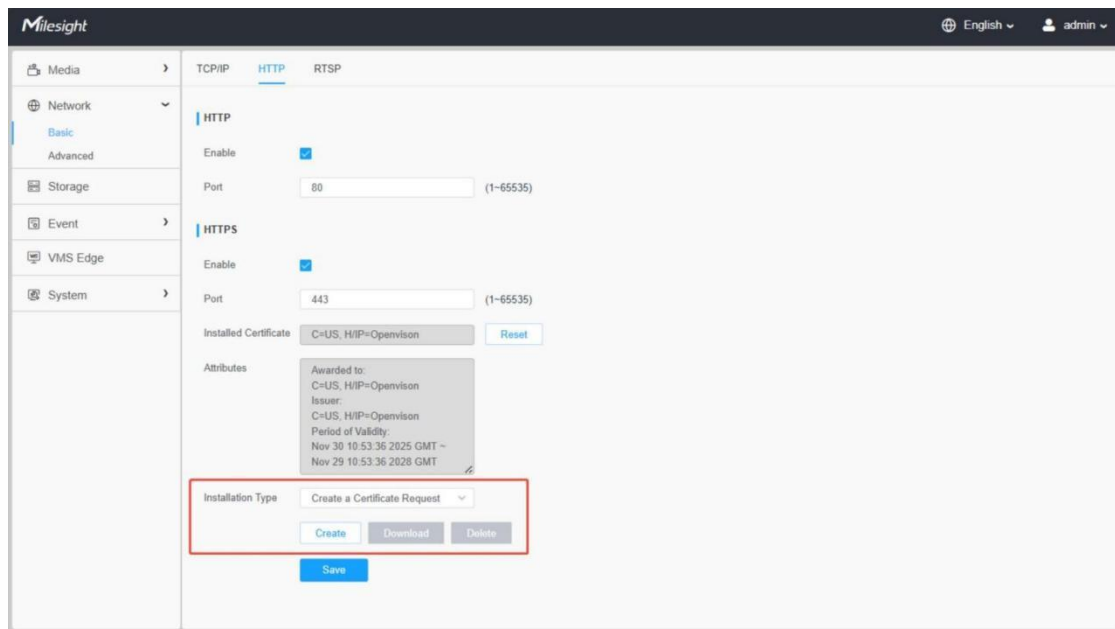


- Create a Certificate Request:

Firstly, click “Create” button. And then enter Country, Common Name and other information to create the certificate request;

Download the certificate request and submit it to the trusted certificate authority for signature;

After receiving the signed valid certificate, import the certificate to the device.



After creating and installing the certificate successfully, you can check the certificate information and reset the information on the following interface. And you can access the OpenVision Server by inputting <https://ip:port> via the web browser.

6.3.1.3 RTSP

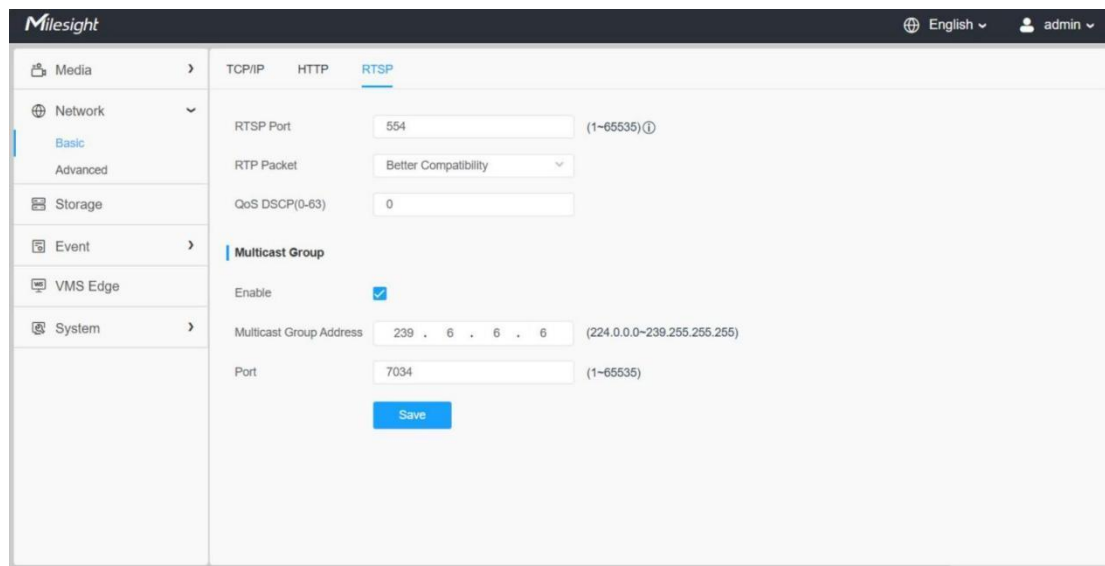


Table 8. Description of the buttons

Parameters	Function Introduction
------------	-----------------------

RTSP Port	The port of RTSP, the default is 554.	
RTP Packet	There are Better Compatibility and Better Performance two options, if your camera's image mess up, please switch this option.	
QoS DSCP	The valid value range of the DSCP is 0-63.	
Multicast Group	Enable	Enable or disable the Multicast Group feature.
	Multicast Group Address	Support multicast function.
	Port	The port of multicast group, the default is 7034. The valid value range of the port is 1-65535.
	Save the configuration.	

**Note:**

- ✓ DSCP refers to the Differentiated Service Code Point; and the DSCP value is used in the IP header to indicate the priority of the data.
- A reboot is required for the settings to take effect.

6.3.2 Advanced

6.3.2.1 ONVIF

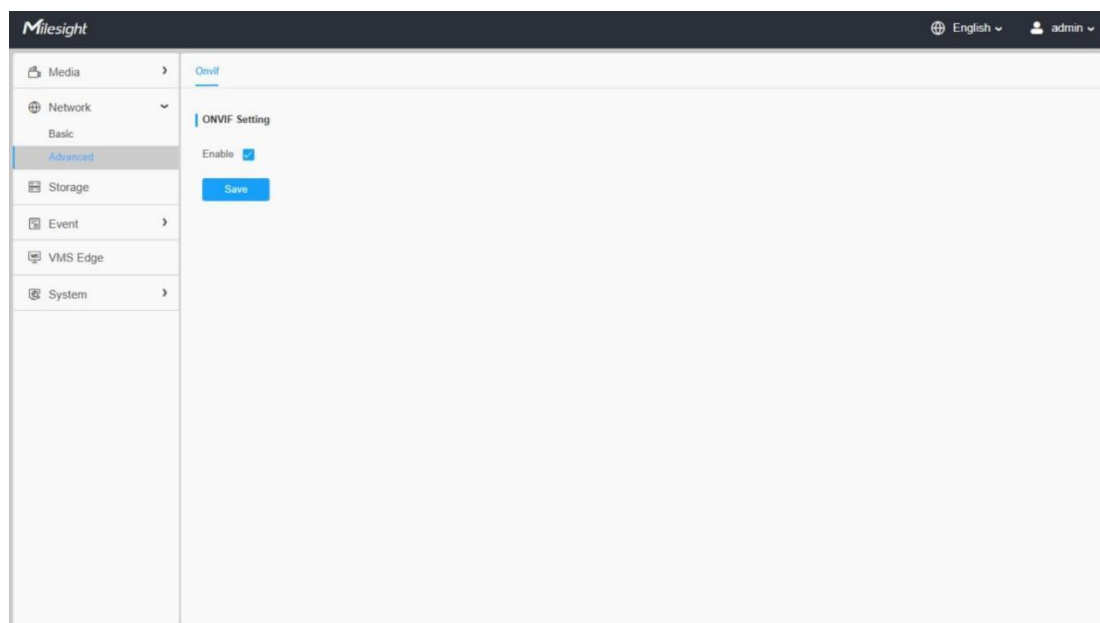


Table 9. Description of the buttons

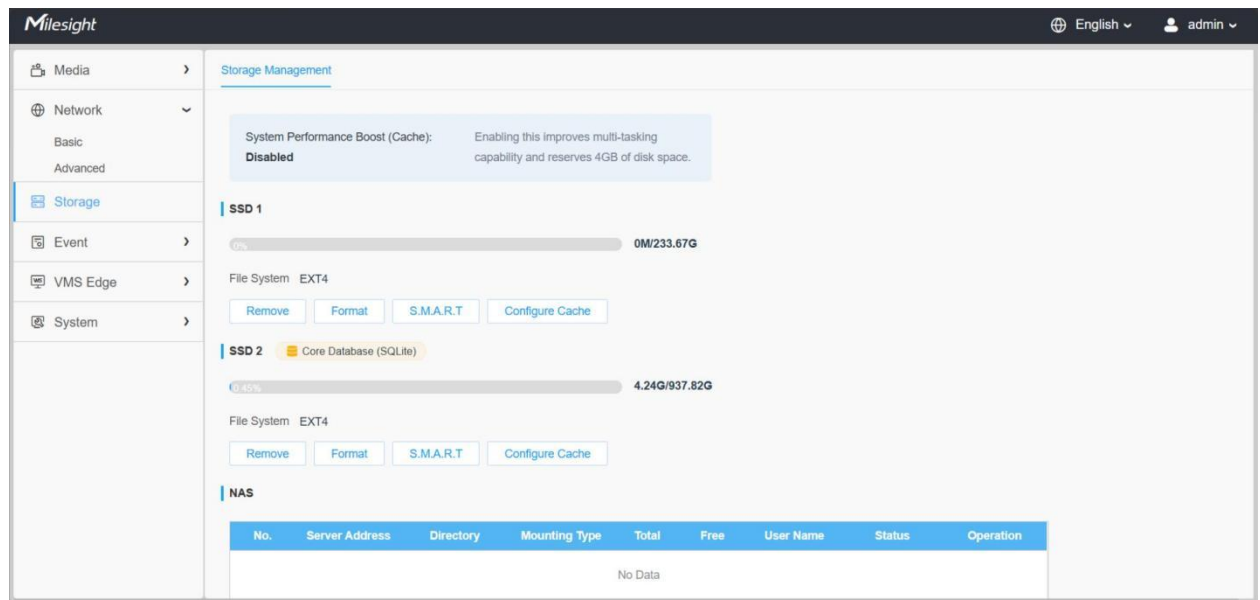
Parameters	Function Introduction
ONVIF Setting	Here you can choose whether to enable or disable the ONVIF function. If the ONVIF function is enabled, it can be searched out, added and connected by third-party software through ONVIF protocols. Generally, the default status of ONVIF function is enabled.

6.4 Storage

The Storage Management module differs between SE0216R and SE0232R.

6.4.1 Storage Management (for SE0216R)

Step 1: Ensure your OpenVision Server has been installed and the HDD/SSD has been initialized, please check it on “Storage” -> “Storage Management” interface.



After that, it will be automatically detected, and the detailed information of the HDD/SSD will be displayed on the HDD/SSD bar.

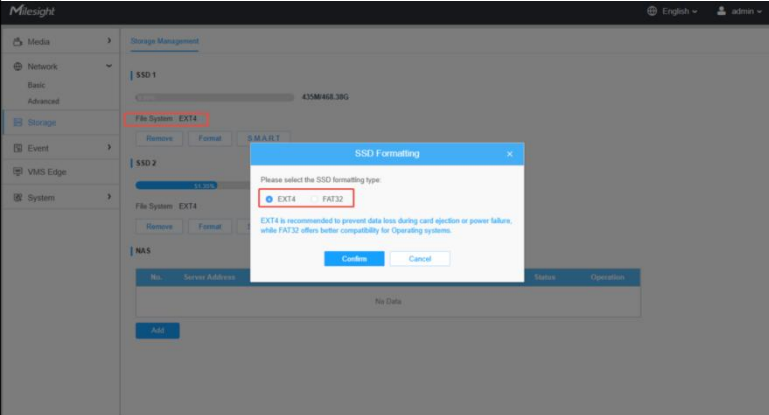
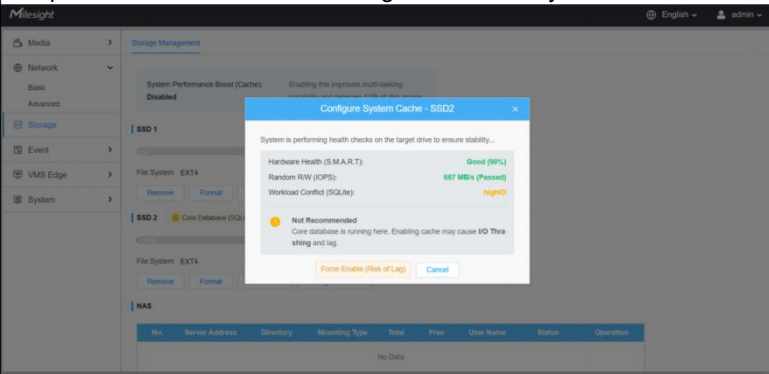
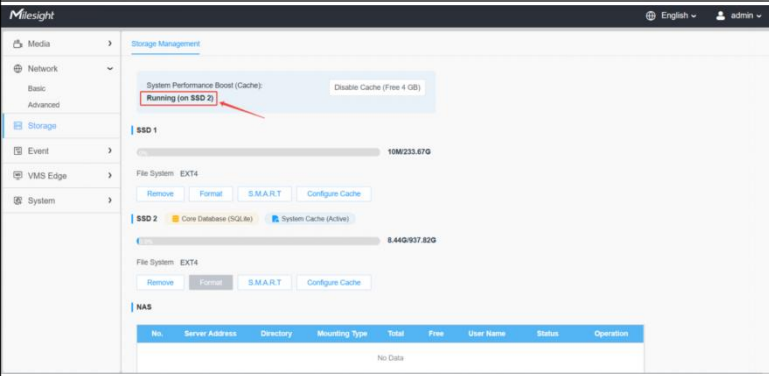
Step 2: In the HDD/SSD bar, you can remove, format, check the health status, or configure the cache of HDD/SSD.

[Warnings]:

- To ensure proper access, please always format the HDD/SSD via the Web interface!
- Never format the HDD/SSD from the Ubuntu desktop using the “system” user account!

Table 10. Description of the buttons

Parameters	Function Introduction
HDD/SSD	Format: Click to format HDD/SSD, the files in HDD/SSD will be removed. EXT4 file system is supported. Only for Unassigned + READY disks.

	 Remove: Click to remove HDD/SSD. S.M.A.R.T: Click to check health information. Configure Cache: Click to configure the selected HDD/SSD as a system cache drive. This reserves 4GB of disk space to improve multi-tasking performance, making operations like recording, playback, and export feel smoother when running simultaneously.  
NAS	The network disk should be available within the network and properly configured to store the recorded files, etc. NAS (Network-Attached Storage), connecting the storage devices to the existing network, provides data and files services.

Add ✕

Server Address*

Directory*

Mounting Type NFS ▼

Save
Cancel

Server Address: IP address of NAS server.

Directory: Input the NAS directory, e.g. “\path”.

Mounting Type: NFS and SMB/CIFS are available. And you can set the user name and password to guarantee the security if SMB/CIFS is selected.

Note:

- Up to 5 NAS disks can be connected.
- For more details about how to use NAS on Milesight devices, please refer to <https://milesight.freshdesk.com/a/solutions/articles/69000797902>.

6.4.2 Storage Management (for SE0232R)

The screenshot displays the Milesight Storage Management interface. The top navigation bar includes 'Media', 'Network', 'Storage' (selected), 'Event', 'VMS Edge', and 'System'. The 'Storage' section is active, showing 'Storage Management' and 'NAS'.

System Performance Boost (Cache): Running (on raid1-197) Disable Cache

raid1-197 System Cache (Active) ONLINE RAID 1 Mirror Low Memory Mode Healthy and writable.

Usable Capacity: 920.0GB | Usage: 1% | Topology: mirror-0 | Recordsize: 1024 KB

VDI / Device	Status	Physical Location	Operation
mirror-0 TOSHIBA DT01ABA1	ONLINE	SATA1 (TOSHIBA DT01ABA1)	
mirror-0 TOSHIBA DT01ABA1	ONLINE	SATA2 (TOSHIBA DT01ABA1)	

Configure Cache Pool Settings

Physical Disks Inventory Slot, device role, health state, and allowed operations are synchronized with the pool lifecycle.

Inventory Pool Protected Pool Type: RAID 1 Low Memory Mode Active Protected Storage Workflow Pool Protected

Slot	Device	Type	Capacity	Disk Details	Pool Role	Status	Health	Operation
SATA1	TOSHIBA DT01ABA1	HDD	920.0 GB	904.3 GB / 920.0 GB 99% Available	Member	ONLINE	SMART Passed	
SATA2	TOSHIBA DT01ABA1	HDD	920.0 GB	904.3 GB / 920.0 GB 99% Available	Member	ONLINE	SMART Passed	
SSD 1 (NGFF1)	NS1T06SSD530	SSD	937.8 GB	921.6 GB / 937.8 GB 98% Available	Unassigned	READY	SMART Passed	
SSD 2 (NGFF3)	KINGSTON SNV5S1000G	SSD	915.8 GB	896.8 GB / 915.8 GB 97% Available	Unassigned	READY	SMART Passed	
	NS1T06SSD530	SSD	937.8 GB	923.5 GB / 937.8 GB	Unassigned	READY	SMART Passed	

(1) Overview

The Storage Manager page consists of two main sections:

- **Storage Pool (Upper Section):** Displays the logical RAID1 pool status, capacity, member mapping, and maintenance actions.
- **Physical Disks Inventory (Lower Section):** Displays all physical disk slots, models, capacities, pool roles, statuses, health, and available operations.

(2) Creating a RAID1 Storage Pool

The device supports RAID1 configuration for dual HDD setups on 32-channel models (SE0232R-K), providing data redundancy and protection against single-disk failure. Single-disk models do not support RAID configuration.

When no storage pool exists, the system displays an empty state card with the message "No Storage Pool Detected" and a "+ Create Storage Pool" button.

Prerequisites:

At least 2 compatible disks must be installed

Disks must be in Unassigned + READY state

Disks with capacity mismatch are visible but disabled (marked as "Mismatch")

Steps:

Step 1: Click "+ Create Storage Pool" to open the creation dialog.

Step 2: Enter the pool name:

Step 3: Select at least 2 compatible disks from the candidate list.

Step 4: Review the System Profile section (read-only):

Step 5: Check the mandatory Data Loss Warning checkbox:

⚠ Warning: The Create Pool button remains disabled until the data erasure confirmation is checked.

Step 6: Click "Create Pool".

Post-Creation: Upon success, the pool enters ONLINE state. If creation fails, temporary resources are rolled back and an error is logged.

(3) RAID1 Status and State Machine

The RAID1 storage pool operates through the following states:

Status	Description
ONLINE	Both disks operational, data fully synchronized. Pool functioning normally.
Scrubbing	Data scrubbing (patrol read) in progress. System verifies data integrity by reading all blocks and comparing mirrored copies.
DEGRADED	One disk failed or removed. RAID operating with reduced redundancy. Data accessible from healthy disk.
Awaiting Repair	Replacement disk inserted but rebuild not yet started. Pool remains DEGRADED.
RESILVERING	System actively rebuilding data from healthy disk to replacement disk.
Repair Failed	Rebuild process failed. Pool returns to DEGRADED.

State Flow:

No Pool → Create Pool → ONLINE ↔ Scrubbing



DEGRADED → Insert Disk → Awaiting Repair



RESILVERING ← Confirm Repair



Success: ONLINE / Failure: DEGRADED

Data Scrubbing (Patrol Read):

Configuration:

Step 1: Navigate to Storage → Storage Management → Pool Setting.

Step 2: Configure Scrub Schedule:

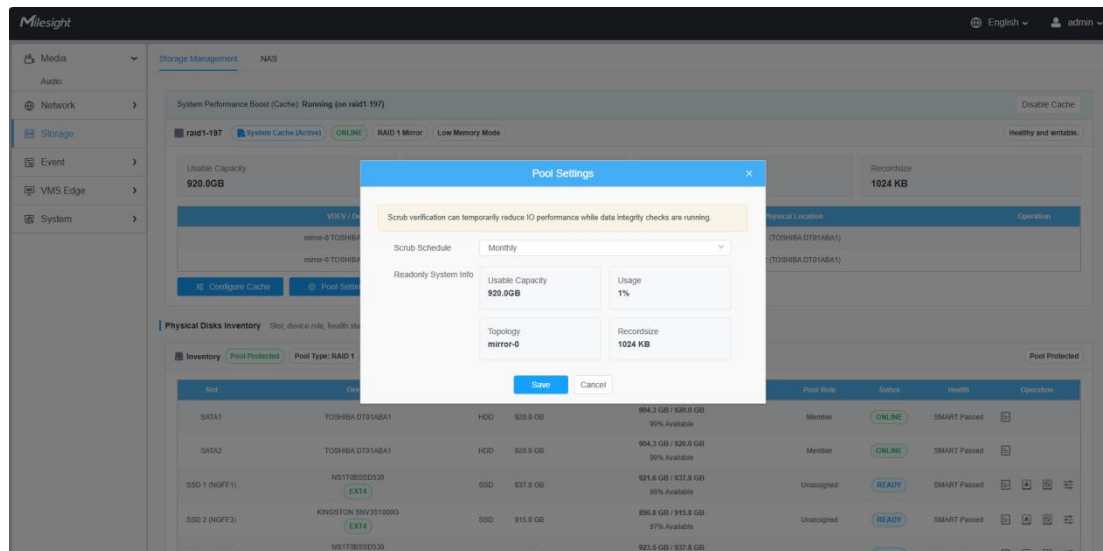
Options: Monthly / Weekly

Default: Monthly

Step 3: Click "Save".

Scrub Results:

Success: Pool returns to ONLINE



Degraded Mode and Repair:

When a disk fails or is removed:

- Pool status changes to DEGRADED
- Logical member mapping shows failed disk as UNAVAIL
- Physical disk list shows original slot as EMPTY
- High-risk actions are locked

Repair Process:

Step 1: Insert a compatible replacement disk.

Step 2: The system validates the replacement disk:

- Must be Unassigned + READY
- Must meet minimum capacity requirements
- Must not have write protection, third-party signatures, or residual partitions

Step 3: If validation passes, disk shows as Candidate Ready. Click "Repair" to open the Repair Pool: Select Replacement dialog.

Step 4: Select the replacement disk from the candidate list:

Insufficient capacity disks show "Too Small" and are disabled

Step 5: Review the warning: "The selected disk will be erased. Repair will start immediately and enter rebuild."

Step 6: Click "Confirm & Repair".

Rebuild Completion:

Success: Pool returns to ONLINE, redundancy restored

Failure: Pool returns to DEGRADED, error logged, failed disk marked as Failed Candidate

⚠ Important: Do not power off or remove disks during rebuild. Interruption may result in data loss or require restarting the rebuild.

Foreign RAID1 Recovery:

When disks with existing RAID metadata from another Milesight device are inserted, the system detects them as foreign RAID members.

Detection Scenarios:

Scenario	Available Actions	Recovery Process
Single Foreign Member	Recover RAID Group, View Disk Info, Format	Step 1: Click "Recover RAID Group". Step 2: Review the confirmation dialog Next Action: Repair required to restore redundancy Step 4: Click "Confirm & Recover". Result: The foreign member is imported as a DEGRADED pool. You must insert a compatible disk and perform Repair to restore redundancy
Multiple Foreign Groups	Select one group to recover, or clear others	System displays conflict warning: "Do not merge groups" Select one group to recover Other foreign disks must be Formatted or cleared before Repair becomes available After clearing other foreign signatures, message: "Foreign signature cleared. Candidate ready for Repair."
Complete Foreign Group (both members)	Recover RAID Group	Both members detected from same foreign pool Click "Recover RAID Group" to import as ONLINE pool Both members immediately become locked local member disks

(4) Physical Disk Management

The Physical Disks Inventory table displays:

Column	Description
Slot	Physical slot identifier (SATA1, SATA2, SSD 1/2)
Device	Disk manufacturer and model (empty slots show "No Device")
Type	Display type as HDD or SSD.
Capacity	Total physical disk capacity
Disk Details	Available/Total space and Available % (e.g., "8.2 TB / 10.0 TB, 82% Available")
Pool Role	Member / Unassigned
Status	READY / EMPTY / REBUILDING / Damaged / Unformatted
Health	SMART Passed / SMART Warning / Unknown
Operation	View Info / Remove / Format / Configure Cache

Available Operations:

Slot	Device	Type	Capacity	Disk Details	Pool Role	Status	Health	Operation
SATA1	TOSHIBA DT01ABA1	HDD	920.0 GB	904.3 GB / 920.0 GB 99% Available	Member	ONLINE	SMART Passed	
SATA2	TOSHIBA DT01ABA1	HDD	920.0 GB	904.3 GB / 920.0 GB 99% Available	Member	ONLINE	SMART Passed	
SSD 1 (NGFF1)	NS1T08SSD530 EXT4	SSD	937.8 GB	921.6 GB / 937.8 GB 98% Available	Unassigned	READY	SMART Passed	
SSD 2 (NGFF3)	KINGSTON SNV351000G EXT4	SSD	915.8 GB	896.8 GB / 915.8 GB 97% Available	Unassigned	READY	SMART Passed	
SSD 3 (NGFF2)	NS1T08SSD530 EXT4 Core Database (SQLite)	SSD	937.8 GB	923.5 GB / 937.8 GB 98% Available	Unassigned	READY	SMART Passed	

Parameters	Function Introduction
------------	-----------------------

	Format: Click to format HDD/SSD, the files in HDD/SSD will be removed. EXT4 file system is supported. Only for Unassigned + READY disks.																								
	Remove: Click to remove HDD/SSD. Only for Unassigned + READY disks.																								
	View Info: Click to check HDD/SSD health information. Disk Details (SSD 1 (NGFF1)) <table><thead><tr><th colspan="2">Hardware</th><th colspan="2">Health</th></tr></thead><tbody><tr><td>Model</td><td>NS1T0BSSD530</td><td>SMART</td><td>Passed</td></tr><tr><td>Serial</td><td>Y5FT004413T</td><td>Temp</td><td>39°C</td></tr><tr><td>Capacity</td><td>937.8 GB</td><td>Life</td><td>100%</td></tr><tr><td>Sector</td><td>512 / 512</td><td>Last Health Update</td><td>2026-09-13 19:54:12</td></tr><tr><td></td><td></td><td>Recent Alerts</td><td>No recent alerts.</td></tr></tbody></table> Close	Hardware		Health		Model	NS1T0BSSD530	SMART	Passed	Serial	Y5FT004413T	Temp	39°C	Capacity	937.8 GB	Life	100%	Sector	512 / 512	Last Health Update	2026-09-13 19:54:12			Recent Alerts	No recent alerts.
Hardware		Health																							
Model	NS1T0BSSD530	SMART	Passed																						
Serial	Y5FT004413T	Temp	39°C																						
Capacity	937.8 GB	Life	100%																						
Sector	512 / 512	Last Health Update	2026-09-13 19:54:12																						
		Recent Alerts	No recent alerts.																						
	Configure Cache: Click to configure the selected HDD/SSD as a system cache drive. This reserves 4GB of disk space to improve multi-tasking performance, making operations like recording, playback, and export feel smoother when running simultaneously. Configure System Cache - SSD2 System is performing health checks on the target drive to ensure stability... Hardware Health (S.M.A.R.T): Good (95%) Random RW (IOPS): 687 MB/s (Passed) Workload Conflict (SQLite): High Not Recommended Core database is running here. Enabling cache may cause I/O Throttling and lag. Force Enable (Risk of Lag) Cancel Storage Management System Performance Boost (Caches): Enabling this improves multi-tasking performance, but it may cause I/O Throttling and lag. Disabled Configure System Cache - SSD2 <table><thead><tr><th>No.</th><th>Server Address</th><th>Directory</th><th>Mounting Type</th><th>Total</th><th>Free</th><th>User Name</th><th>Status</th><th>Operations</th></tr></thead><tbody><tr><td colspan="9">No Data</td></tr></tbody></table> Storage Management System Performance Boost (Caches): Reserving 4GB (10%) Cache Size: 4GB (10%) Cache Type: SSD1 (10%) Cache Type: SSD2 (10%) Cache Type: SSD3 (10%) Cache Type: SSD4 (10%) Cache Type: SSD5 (10%) Cache Type: SSD6 (10%) Cache Type: SSD7 (10%) Cache Type: SSD8 (10%) Cache Type: SSD9 (10%) Cache Type: SSD10 (10%) Cache Type: SSD11 (10%) Cache Type: SSD12 (10%) Cache Type: SSD13 (10%) Cache Type: SSD14 (10%) Cache Type: SSD15 (10%) Cache Type: SSD16 (10%) Cache Type: SSD17 (10%) Cache Type: SSD18 (10%) Cache Type: SSD19 (10%) Cache Type: SSD20 (10%) Cache Type: SSD21 (10%) Cache Type: SSD22 (10%) Cache Type: SSD23 (10%) Cache Type: SSD24 (10%) Cache Type: SSD25 (10%) Cache Type: SSD26 (10%) Cache Type: SSD27 (10%) Cache Type: SSD28 (10%) Cache Type: SSD29 (10%) Cache Type: SSD30 (10%) Cache Type: SSD31 (10%) Cache Type: SSD32 (10%) Cache Type: SSD33 (10%) Cache Type: SSD34 (10%) Cache Type: SSD35 (10%) Cache Type: SSD36 (10%) Cache Type: SSD37 (10%) Cache Type: SSD38 (10%) Cache Type: SSD39 (10%) Cache Type: SSD40 (10%) Cache Type: SSD41 (10%) Cache Type: SSD42 (10%) Cache Type: SSD43 (10%) Cache Type: SSD44 (10%) Cache Type: SSD45 (10%) Cache Type: SSD46 (10%) Cache Type: SSD47 (10%) Cache Type: SSD48 (10%) Cache Type: SSD49 (10%) Cache Type: SSD50 (10%) Cache Type: SSD51 (10%) Cache Type: SSD52 (10%) Cache Type: SSD53 (10%) Cache Type: SSD54 (10%) Cache Type: SSD55 (10%) Cache Type: SSD56 (10%) Cache Type: SSD57 (10%) Cache Type: SSD58 (10%) Cache Type: SSD59 (10%) Cache Type: SSD60 (10%) Cache Type: SSD61 (10%) Cache Type: SSD62 (10%) Cache Type: SSD63 (10%) Cache Type: SSD64 (10%) Cache Type: SSD65 (10%) Cache Type: SSD66 (10%) Cache Type: SSD67 (10%) Cache Type: SSD68 (10%) Cache Type: SSD69 (10%) Cache Type: SSD70 (10%) Cache Type: SSD71 (10%) Cache Type: SSD72 (10%) Cache Type: SSD73 (10%) Cache Type: SSD74 (10%) Cache Type: SSD75 (10%) Cache Type: SSD76 (10%) Cache Type: SSD77 (10%) Cache Type: SSD78 (10%) Cache Type: SSD79 (10%) Cache Type: SSD80 (10%) Cache Type: SSD81 (10%) Cache Type: SSD82 (10%) Cache Type: SSD83 (10%) Cache Type: SSD84 (10%) Cache Type: SSD85 (10%) Cache Type: SSD86 (10%) Cache Type: SSD87 (10%) Cache Type: SSD88 (10%) Cache Type: SSD89 (10%) Cache Type: SSD90 (10%) Cache Type: SSD91 (10%) Cache Type: SSD92 (10%) Cache Type: SSD93 (10%) Cache Type: SSD94 (10%) Cache Type: SSD95 (10%) Cache Type: SSD96 (10%) Cache Type: SSD97 (10%) Cache Type: SSD98 (10%) Cache Type: SSD99 (10%) Cache Type: SSD100 (10%) Cache Type: SSD101 (10%) Cache Type: SSD102 (10%) Cache Type: SSD103 (10%) Cache Type: SSD104 (10%) Cache Type: SSD105 (10%) Cache Type: SSD106 (10%) Cache Type: SSD107 (10%) Cache Type: SSD108 (10%) Cache Type: SSD109 (10%) Cache Type: SSD110 (10%) Cache Type: SSD111 (10%) Cache Type: SSD112 (10%) Cache Type: SSD113 (10%) Cache Type: SSD114 (10%) Cache Type: SSD115 (10%) Cache Type: SSD116 (10%) Cache Type: SSD117 (10%) Cache Type: SSD118 (10%) Cache Type: SSD119 (10%) Cache Type: SSD120 (10%) Cache Type: SSD121 (10%) Cache Type: SSD122 (10%) Cache Type: SSD123 (10%) Cache Type: SSD124 (10%) Cache Type: SSD125 (10%) Cache Type: SSD126 (10%) Cache Type: SSD127 (10%) Cache Type: SSD128 (10%) Cache Type: SSD129 (10%) Cache Type: SSD130 (10%) Cache Type: SSD131 (10%) Cache Type: SSD132 (10%) Cache Type: SSD133 (10%) Cache Type: SSD134 (10%) Cache Type: SSD135 (10%) Cache Type: SSD136 (10%) Cache Type: SSD137 (10%) Cache Type: SSD138 (10%) Cache Type: SSD139 (10%) Cache Type: SSD140 (10%) Cache Type: SSD141 (10%) Cache Type: SSD142 (10%) Cache Type: SSD143 (10%) Cache Type: SSD144 (10%) Cache Type: SSD145 (10%) Cache Type: SSD146 (10%) Cache Type: SSD147 (10%) Cache Type: SSD148 (10%) Cache Type: SSD149 (10%) Cache Type: SSD150 (10%) Cache Type: SSD151 (10%) Cache Type: SSD152 (10%) Cache Type: SSD153 (10%) Cache Type: SSD154 (10%) Cache Type: SSD155 (10%) Cache Type: SSD156 (10%) Cache Type: SSD157 (10%) Cache Type: SSD158 (10%) Cache Type: SSD159 (10%) Cache Type: SSD160 (10%) Cache Type: SSD161 (10%) Cache Type: SSD162 (10%) Cache Type: SSD163 (10%) Cache Type: SSD164 (10%) Cache Type: SSD165 (10%) Cache Type: SSD166 (10%) Cache Type: SSD167 (10%) Cache Type: SSD168 (10%) Cache Type: SSD169 (10%) Cache Type: SSD170 (10%) Cache Type: SSD171 (10%) Cache Type: SSD172 (10%) Cache Type: SSD173 (10%) Cache Type: SSD174 (10%) Cache Type: SSD175 (10%) Cache Type: SSD176 (10%) Cache Type: SSD177 (10%) Cache Type: SSD178 (10%) Cache Type: SSD179 (10%) Cache Type: SSD180 (10%) Cache Type: SSD181 (10%) Cache Type: SSD182 (10%) Cache Type: SSD183 (10%) Cache Type: SSD184 (10%) Cache Type: SSD185 (10%) Cache Type: SSD186 (10%) Cache Type: SSD187 (10%) Cache Type: SSD188 (10%) Cache Type: SSD189 (10%) Cache Type: SSD190 (10%) Cache Type: SSD191 (10%) Cache Type: SSD192 (10%) Cache Type: SSD193 (10%) Cache Type: SSD194 (10%) Cache Type: SSD195 (10%) Cache Type: SSD196 (10%) Cache Type: SSD197 (10%) Cache Type: SSD198 (10%) Cache Type: SSD199 (10%) Cache Type: SSD200 (10%) Cache Type: SSD201 (10%) Cache Type: SSD202 (10%) Cache Type: SSD203 (10%) Cache Type: SSD204 (10%) Cache Type: SSD205 (10%) Cache Type: SSD206 (10%) Cache Type: SSD207 (10%) Cache Type: SSD208 (10%) Cache Type: SSD209 (10%) Cache Type: SSD210 (10%) Cache Type: SSD211 (10%) Cache Type: SSD212 (10%) Cache Type: SSD213 (10%) Cache Type: SSD214 (10%) Cache Type: SSD215 (10%) Cache Type: SSD216 (10%) Cache Type: SSD217 (10%) Cache Type: SSD218 (10%) Cache Type: SSD219 (10%) Cache Type: SSD220 (10%) Cache Type: SSD221 (10%) Cache Type: SSD222 (10%) Cache Type: SSD223 (10%) Cache Type: SSD224 (10%) Cache Type: SSD225 (10%) Cache Type: SSD226 (10%) Cache Type: SSD227 (10%) Cache Type: SSD228 (10%) Cache Type: SSD229 (10%) Cache Type: SSD230 (10%) Cache Type: SSD231 (10%) Cache Type: SSD232 (10%) Cache Type: SSD233 (10%) Cache Type: SSD234 (10%) Cache Type: SSD235 (10%) Cache Type: SSD236 (10%) Cache Type: SSD237 (10%) Cache Type: SSD238 (10%) Cache Type: SSD239 (10%) Cache Type: SSD240 (10%) Cache Type: SSD241 (10%) Cache Type: SSD242 (10%) Cache Type: SSD243 (10%) Cache Type: SSD244 (10%) Cache Type: SSD245 (10%) Cache Type: SSD246 (10%) Cache Type: SSD247 (10%) Cache Type: SSD248 (10%) Cache Type: SSD249 (10%) Cache Type: SSD250 (10%) Cache Type: SSD251 (10%) Cache Type: SSD252 (10%) Cache Type: SSD253 (10%) Cache Type: SSD254 (10%) Cache Type: SSD255 (10%) Cache Type: SSD256 (10%) Cache Type: SSD257 (10%) Cache Type: SSD258 (10%) Cache Type: SSD259 (10%) Cache Type: SSD260 (10%) Cache Type: SSD261 (10%) Cache Type: SSD262 (10%) Cache Type: SSD263 (10%) Cache Type: SSD264 (10%) Cache Type: SSD265 (10%) Cache Type: SSD266 (10%) Cache Type: SSD267 (10%) Cache Type: SSD268 (10%) Cache Type: SSD269 (10%) Cache Type: SSD270 (10%) Cache Type: SSD271 (10%) Cache Type: SSD272 (10%) Cache Type: SSD273 (10%) Cache Type: SSD274 (10%) Cache Type: SSD275 (10%) Cache Type: SSD276 (10%) Cache Type: SSD277 (10%) Cache Type: SSD278 (10%) Cache Type: SSD279 (10%) Cache Type: SSD280 (10%) Cache Type: SSD281 (10%) Cache Type: SSD282 (10%) Cache Type: SSD283 (10%) Cache Type: SSD284 (10%) Cache Type: SSD285 (10%) Cache Type: SSD286 (10%) Cache Type: SSD287 (10%) Cache Type: SSD288 (10%) Cache Type: SSD289 (10%) Cache Type: SSD290 (10%) Cache Type: SSD291 (10%) Cache Type: SSD292 (10%) Cache Type: SSD293 (10%) Cache Type: SSD294 (10%) Cache Type: SSD295 (10%) Cache Type: SSD296 (10%) Cache Type: SSD297 (10%) Cache Type: SSD298 (10%) Cache Type: SSD299 (10%) Cache Type: SSD300 (10%) Cache Type: SSD301 (10%) Cache Type: SSD302 (10%) Cache Type: SSD303 (10%) Cache Type: SSD304 (10%) Cache Type: SSD305 (10%) Cache Type: SSD306 (10%) Cache Type: SSD307 (10%) Cache Type: SSD308 (10%) Cache Type: SSD309 (10%) Cache Type: SSD310 (10%) Cache Type: SSD311 (10%) Cache Type: SSD312 (10%) Cache Type: SSD313 (10%) Cache Type: SSD314 (10%) Cache Type: SSD315 (10%) Cache Type: SSD316 (10%) Cache Type: SSD317 (10%) Cache Type: SSD318 (10%) Cache Type: SSD319 (10%) Cache Type: SSD320 (10%) Cache Type: SSD321 (10%) Cache Type: SSD322 (10%) Cache Type: SSD323 (10%) Cache Type: SSD324 (10%) Cache Type: SSD325 (10%) Cache Type: SSD326 (10%) Cache Type: SSD327 (10%) Cache Type: SSD328 (10%) Cache Type: SSD329 (10%) Cache Type: SSD330 (10%) Cache Type: SSD331 (10%) Cache Type: SSD332 (10%) Cache Type: SSD333 (10%) Cache Type: SSD334 (10%) Cache Type: SSD335 (10%) Cache Type: SSD336 (10%) Cache Type: SSD337 (10%) Cache Type: SSD338 (10%) Cache Type: SSD339 (10%) Cache Type: SSD340 (10%) Cache Type: SSD341 (10%) Cache Type: SSD342 (10%) Cache Type: SSD343 (10%) Cache Type: SSD344 (10%) Cache Type: SSD345 (10%) Cache Type: SSD346 (10%) Cache Type: SSD347 (10%) Cache Type: SSD348 (10%) Cache Type: SSD349 (10%) Cache Type: SSD350 (10%) Cache Type: SSD351 (10%) Cache Type: SSD352 (10%) Cache Type: SSD353 (10%) Cache Type: SSD354 (10%) Cache Type: SSD355 (10%) Cache Type: SSD356 (10%) Cache Type: SSD357 (10%) Cache Type: SSD358 (10%) Cache Type: SSD359 (10%) Cache Type: SSD360 (10%) Cache Type: SSD361 (10%) Cache Type: SSD362 (10%) Cache Type: SSD363 (10%) Cache Type: SSD364 (10%) Cache Type: SSD365 (10%) Cache Type: SSD366 (10%) Cache Type: SSD367 (10%) Cache Type: SSD368 (10%) Cache Type: SSD369 (10%) Cache Type: SSD370 (10%) Cache Type: SSD371 (10%) Cache Type: SSD372 (10%) Cache Type: SSD373 (10%) Cache Type: SSD374 (10%) Cache Type: SSD375 (10%) Cache Type: SSD376 (10%) Cache Type: SSD377 (10%) Cache Type: SSD378 (10%) Cache Type: SSD379 (10%) Cache Type: SSD380 (10%) Cache Type: SSD381 (10%) Cache Type: SSD382 (10%) Cache Type: SSD383 (10%) Cache Type: SSD384 (10%) Cache Type: SSD385 (10%) Cache Type: SSD386 (10%) Cache Type: SSD387 (10%) Cache Type: SSD388 (10%) Cache Type: SSD389 (10%) Cache Type: SSD390 (10%) Cache Type: SSD391 (10%) Cache Type: SSD392 (10%) Cache Type: SSD393 (10%) Cache Type: SSD394 (10%) Cache Type: SSD395 (10%) Cache Type: SSD396 (10%) Cache Type: SSD397 (10%) Cache Type: SSD398 (10%) Cache Type: SSD399 (10%) Cache Type: SSD400 (10%) Cache Type: SSD401 (10%) Cache Type: SSD402 (10%) Cache Type: SSD403 (10%) Cache Type: SSD404 (10%) Cache Type: SSD405 (10%) Cache Type: SSD406 (10%) Cache Type: SSD407 (10%) Cache Type: SSD408 (10%) Cache Type: SSD409 (10%) Cache Type: SSD410 (10%) Cache Type: SSD411 (10%) Cache Type: SSD412 (10%) Cache Type: SSD413 (10%) Cache Type: SSD414 (10%) Cache Type: SSD415 (10%) Cache Type: SSD416 (10%) Cache Type: SSD417 (10%) Cache Type: SSD418 (10%) Cache Type: SSD419 (10%) Cache Type: SSD420 (10%) Cache Type: SSD421 (10%) Cache Type: SSD422 (10%) Cache Type: SSD423 (10%) Cache Type: SSD424 (10%) Cache Type: SSD425 (10%) Cache Type: SSD426 (10%) Cache Type: SSD427 (10%) Cache Type: SSD428 (10%) Cache Type: SSD429 (10%) Cache Type: SSD430 (10%) Cache Type: SSD431 (10%) Cache Type: SSD432 (10%) Cache Type: SSD433 (10%) Cache Type: SSD434 (10%) Cache Type: SSD435 (10%) Cache Type: SSD436 (10%) Cache Type: SSD437 (10%) Cache Type: SSD438 (10%) Cache Type: SSD439 (10%) Cache Type: SSD440 (10%) Cache Type: SSD441 (10%) Cache Type: SSD442 (10%) Cache Type: SSD443 (10%) Cache Type: SSD444 (10%) Cache Type: SSD445 (10%) Cache Type: SSD446 (10%) Cache Type: SSD447 (10%) Cache Type: SSD448 (10%) Cache Type: SSD449 (10%) Cache Type: SSD450 (10%) Cache Type: SSD451 (10%) Cache Type: SSD452 (10%) Cache Type: SSD453 (10%) Cache Type: SSD454 (10%) Cache Type: SSD455 (10%) Cache Type: SSD456 (10%) Cache Type: SSD457 (10%) Cache Type: SSD458 (10%) Cache Type: SSD459 (10%) Cache Type: SSD460 (10%) Cache Type: SSD461 (10%) Cache Type: SSD462 (10%) Cache Type: SSD463 (10%) Cache Type: SSD464 (10%) Cache Type: SSD465 (10%) Cache Type: SSD466 (10%) Cache Type: SSD467 (10%) Cache Type: SSD468 (10%) Cache Type: SSD469 (10%) Cache Type: SSD470 (10%) Cache Type: SSD471 (10%) Cache Type: SSD472 (10%) Cache Type: SSD473 (10%) Cache Type: SSD474 (10%) Cache Type: SSD475 (10%) Cache Type: SSD476 (10%) Cache Type: SSD477 (10%) Cache Type: SSD478 (10%) Cache Type: SSD479 (10%) Cache Type: SSD480 (10%) Cache Type: SSD481 (10%) Cache Type: SSD482 (10%) Cache Type: SSD483 (10%) Cache Type: SSD484 (10%) Cache Type: SSD485 (10%) Cache Type: SSD486 (10%) Cache Type: SSD487 (10%) Cache Type: SSD488 (10%) Cache Type: SSD489 (10%) Cache Type: SSD490 (10%) Cache Type: SSD491 (10%) Cache Type: SSD492 (10%) Cache Type: SSD493 (10%) Cache Type: SSD494 (10%) Cache Type: SSD495 (10%) Cache Type: SSD496 (10%) Cache Type: SSD497 (10%) Cache Type: SSD498 (10%) Cache Type: SSD499 (10%) Cache Type: SSD500 (10%) Cache Type: SSD501 (10%) Cache Type: SSD502 (10%) Cache Type: SSD503 (10%) Cache Type: SSD504 (10%) Cache Type: SSD505 (10%) Cache Type: SSD506 (10%) Cache Type: SSD507 (10%) Cache Type: SSD508 (10%) Cache Type: SSD509 (10%) Cache Type: SSD510 (10%) Cache Type: SSD511 (10%) Cache Type: SSD512 (10%) Cache Type: SSD513 (10%) Cache Type: SSD514 (10%) Cache Type: SSD515 (10%) Cache Type: SSD516 (10%) Cache Type: SSD517 (10%) Cache Type: SSD518 (10%) Cache Type: SSD519 (10%) Cache Type: SSD520 (10%) Cache Type: SSD521 (10%) Cache Type: SSD522 (10%) Cache Type: SSD523 (10%) Cache Type: SSD524 (10%) Cache Type: SSD525 (10%) Cache Type: SSD526 (10%) Cache Type: SSD527 (10%) Cache Type: SSD528 (10%) Cache Type: SSD529 (10%) Cache Type: SSD530 (10%) Cache Type: SSD531 (10%) Cache Type: SSD532 (10%) Cache Type: SSD533 (10%) Cache Type: SSD534 (10%) Cache Type: SSD535 (10%) Cache Type: SSD536 (10%) Cache Type: SSD537 (10%) Cache Type: SSD538 (10%) Cache Type: SSD539 (10%) Cache Type: SSD540 (10%) Cache Type: SSD541 (10%) Cache Type: SSD542 (10%) Cache Type: SSD543 (10%) Cache Type: SSD544 (10%) Cache Type: SSD545 (10%) Cache Type: SSD546 (10%) Cache Type: SSD547 (10%) Cache Type: SSD548 (10%) Cache Type: SSD549 (10%) Cache Type: SSD550 (10%) Cache Type: SSD551 (10%) Cache Type: SSD552 (10%) Cache Type: SSD553 (10%) Cache Type: SSD554 (10%) Cache Type: SSD555 (10%) Cache Type: SSD556 (10%) Cache Type: SSD557 (10%) Cache Type: SSD558 (10%) Cache Type: SSD559 (10%) Cache Type: SSD560 (10%) Cache Type: SSD561 (10%) Cache Type: SSD562 (10%) Cache Type: SSD563 (10%) Cache Type: SSD564 (10%) Cache Type: SSD565 (10%) Cache Type: SSD566 (10%) Cache Type: SSD567 (10%) Cache Type: SSD568 (10%) Cache Type: SSD569 (10%) Cache Type: SSD570 (10%) Cache Type: SSD571 (10%) Cache Type: SSD572 (10%) Cache Type: SSD573 (10%) Cache Type: SSD574 (10%) Cache Type: SSD575 (10%) Cache Type: SSD576 (10%) Cache Type: SSD577 (10%) Cache Type: SSD578 (10%) Cache Type: SSD579 (10%) Cache Type: SSD580 (10%) Cache Type: SSD581 (10%) Cache Type: SSD582 (10%) Cache Type: SSD583 (10%) Cache Type: SSD584 (10%) Cache Type: SSD585 (10%) Cache Type: SSD586 (10%) Cache Type: SSD587 (10%) Cache Type: SSD588 (10%) Cache Type: SSD589 (10%) Cache Type: SSD590 (10%) Cache Type: SSD591 (10%) Cache Type: SSD592 (10%) Cache Type: SSD593 (10%) Cache Type: SSD594 (10%) Cache Type: SSD595 (10%) Cache Type: SSD596 (10%) Cache Type: SSD597 (10%) Cache Type: SSD598 (10%) Cache Type: SSD599 (10%) Cache Type: SSD600 (10%) Cache Type: SSD601 (10%) Cache Type: SSD602 (10%) Cache Type: SSD603 (10%) Cache Type: SSD604 (10%) Cache Type: SSD605 (10%) Cache Type: SSD606 (10%) Cache Type: SSD607 (10%) Cache Type: SSD608 (10%) Cache Type: SSD609 (10%) Cache Type: SSD610 (10%) Cache Type: SSD611 (10%) Cache Type: SSD612 (10%) Cache Type: SSD613 (10%) Cache Type: SSD614 (10%) Cache Type: SSD615 (10%) Cache Type: SSD616 (10%) Cache Type: SSD617 (10%) Cache Type: SSD618 (10%) Cache Type: SSD619 (10%) Cache Type: SSD620 (10%) Cache Type: SSD621 (10%) Cache Type: SSD622 (10%) Cache Type: SSD623 (10%) Cache Type: SSD624 (10%) Cache Type: SSD625 (10%) Cache Type: SSD626 (10%) Cache Type: SSD627 (10%) Cache Type: SSD628 (10%) Cache Type: SSD629 (10%) Cache Type: SSD630 (10%) Cache Type: SSD631 (10%) Cache Type: SSD632 (10%) Cache Type: SSD633 (10%) Cache Type: SSD634 (10%) Cache Type: SSD635 (10%) Cache Type: SSD636 (10%) Cache Type: SSD637 (10%) Cache Type: SSD638 (10%) Cache Type: SSD639 (10%) Cache Type: SSD640 (10%) Cache Type: SSD641 (10%) Cache Type: SSD642 (10%) Cache Type: SSD643 (10%) Cache Type: SSD644 (10%) Cache Type: SSD645 (10%) Cache Type: SSD646 (10%) Cache Type: SSD647 (10%) Cache Type: SSD648 (10%) Cache Type: SSD649 (10%) Cache Type: SSD650 (10%) Cache Type: SSD651 (10%) Cache Type: SSD652 (10%) Cache Type: SSD653 (10%) Cache Type: SSD654 (10%) Cache Type: SSD655 (10%) Cache Type: SSD656 (10%) Cache Type: SSD657 (10%) Cache Type: SSD658 (10%) Cache Type: SSD659 (10%) Cache Type: SSD660 (10%) Cache Type: SSD661 (10%) Cache Type: SSD662 (10%) Cache Type: SSD663 (10%) Cache Type: SSD664 (10%) Cache Type: SSD665 (10%) Cache Type: SSD666 (10%) Cache Type: SSD667 (10%) Cache Type: SSD668 (10%) Cache Type: SSD669 (10%) Cache Type: SSD670 (10%) Cache Type: SSD671 (10%) Cache Type: SSD672 (10%) Cache Type: SSD673 (10%) Cache Type: SSD674 (10%) Cache Type: SSD675 (10%) Cache Type: SSD676 (10%) Cache Type: SSD677 (10%) Cache Type: SSD678 (10%) Cache Type: SSD679 (10%) Cache Type: SSD680 (10%) Cache Type: SSD681 (10%) Cache Type: SSD682 (10%) Cache Type: SSD683 (10%) Cache Type: SSD684 (10%) Cache Type: SSD685 (10%) Cache Type: SSD686 (10%) Cache Type: SSD687 (10%) Cache Type: SSD688 (10%) Cache Type: SSD689 (10%) Cache Type: SSD690 (10%) Cache Type: SSD691 (10%) Cache Type: SSD692 (10%) Cache Type: SSD693 (10%) Cache Type: SSD694 (10%) Cache Type: SSD695 (10%) Cache Type: SSD696 (10%) Cache Type: SSD697 (10%) Cache Type: SSD698 (10%) Cache Type: SSD699 (10%) Cache Type: SSD700 (10%) Cache Type: SSD701 (10%) Cache Type: SSD702 (10%) Cache Type: SSD703 (10%) Cache Type: SSD704 (10%) Cache Type: SSD705 (10%) Cache Type: SSD706 (10%) Cache Type: SSD707 (10%) Cache Type: SSD708 (10%) Cache Type: SSD709 (10%) Cache Type: SSD710 (10%) Cache Type: SSD711 (10%) Cache Type: SSD712 (10%) Cache Type: SSD713 (10%) Cache Type: SSD714 (10%) Cache Type: SSD715 (10%) Cache Type: SSD716 (10%) Cache Type: SSD717 (10%) Cache Type: SSD718 (10%) Cache Type: SSD719 (10%) Cache Type: SSD720 (10%) Cache Type: SSD721 (10%) Cache Type: SSD722 (10%) Cache Type: SSD723 (10%) Cache Type: SSD724 (10%) Cache Type: SSD725 (10%) Cache Type: SSD726 (10%) Cache Type: SSD727 (10%)	No.	Server Address	Directory	Mounting Type	Total	Free	User Name	Status	Operations	No Data														
No.	Server Address	Directory	Mounting Type	Total	Free	User Name	Status	Operations																	
No Data																									

Note: During RESILVERING, Remove and Format buttons display as "Remove Locked" and "Format Locked" and are disabled.

(5) NAS

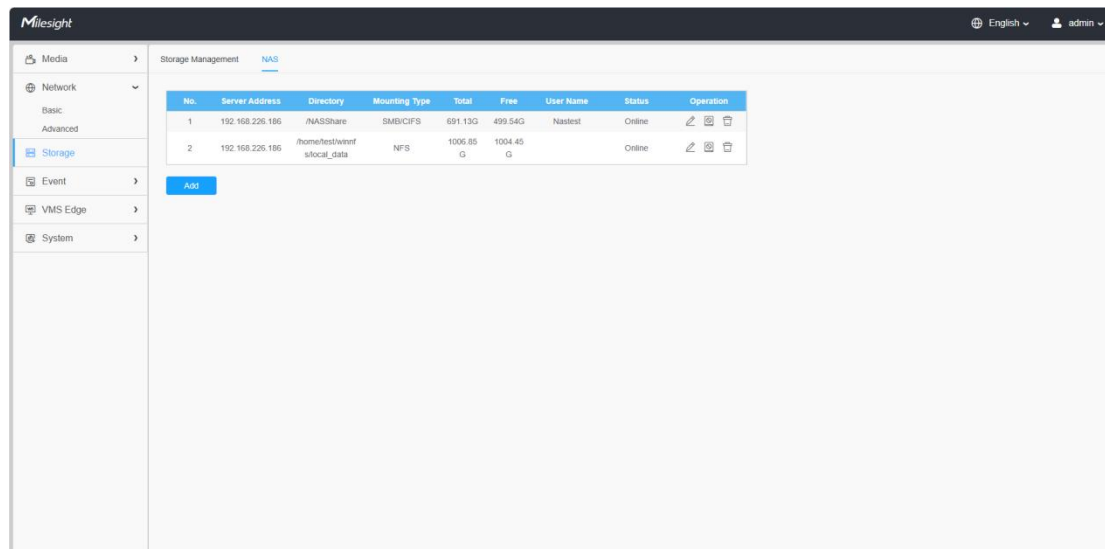


Table 11. Description of the buttons

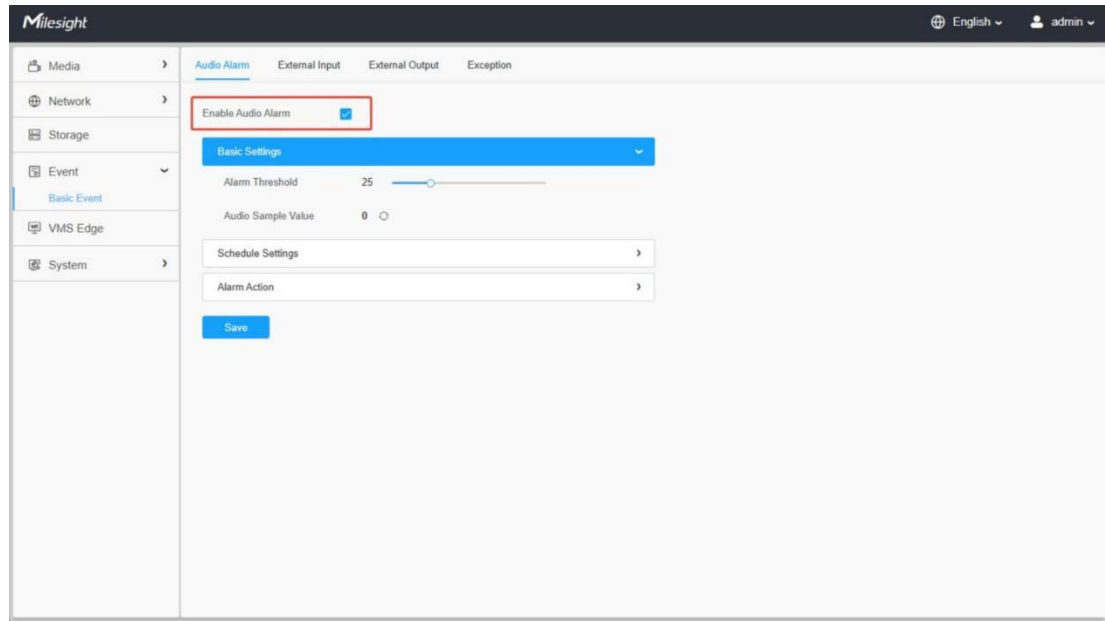
Parameters	Function Introduction
NAS	The network disk should be available within the network and properly configured to store the recorded files, etc. NAS (Network-Attached Storage), connecting the storage devices to the existing network, provides data and files services. Add Server Address* Directory* Mounting Type NFS Save Cancel Server Address: IP address of NAS server. Directory: Input the NAS directory, e.g. "\path". Mounting Type: NFS and SMB/CIFS are available. And you can set the user name and password to guarantee the security if SMB/CIFS is selected. Note: - Up to 5 NAS disks can be connected. - For more details about how to use NAS on Milesight devices, please refer to https://milesight.freshdesk.com/a/solutions/articles/69000797902.

6.5 Event

6.5.1 Basic Event

6.5.1.1 Audio Alarm

Check the check box to enable the Audio Alarm function.



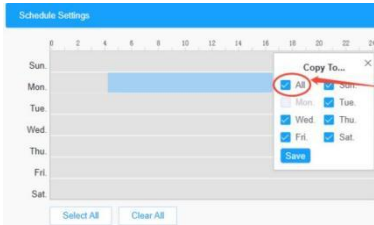
[Basic Settings]

Table 12. Description of the buttons

Parameters	Function Introduction
Alarm Threshold	Audio Alarm will be triggered when the thresholds reaches to a certain value from 0 to 100.
Audio Sample Value	The current value of the audio sample.

[Schedule Settings]

Table 13. Description of the buttons

Parameters	Function Introduction
	Copy the schedule area to another date. The "All" button is handy to copy today's schedule to all days.
	Select all schedule.
	Clear all schedule.

[Alarm Action]

Table 14. Description of the buttons

Parameters	Function Introduction
External Output	If the camera equips with External Output, you can enable the action after configuring the trigger duration. Action Time: Customize/10 seconds/30 seconds/1 minute/5 minutes/Constant are available.
Play Audio	Auto/10 seconds/30 seconds/1 minute/5 minutes/10 minutes are available. 📄 Note: Please enable the Audio Speaker.
HTTP Notification	Support to pop up the alarm news to specified HTTP URL. 📄 Note: - Three HTTP notifications at most can be added to the same event. - HTTP Notification supports Basic & Digest authentication

6.5.1.2 External Input

Step 1: Select External Input number, and enable External Input.

Step 2: Please set the Normal Status firstly, when the Current Status is different with Normal Status, it will lead to the alarm.

Step 3: Set effective time and alarm action for External Input.

Table 15. Description of the buttons

Parameters	Function Introduction
------------	-----------------------

Schedule Settings	Refer to Table 13 for the meanings of the items, here will not repeat again.
Alarm Action	Refer to Table 14 for the meanings of the items, here will not repeat again.

6.5.1.3 External Output

[Normal Status Settings]

Please set the Normal Status firstly, when the Current Status is different with Normal Status, it will lead to the alarm.

[Manual External Output]

You can set the manual external output.

Table 16. Description of the buttons

Parameters	Function Introduction
Manual Output	Click to Start/Stop manual external output.
External Output Action Time	Manual Control/Customize/10 s/1 min./5 min./10 min. are available.

6.5.1.4 Exception

The screenshot shows the Milesight web interface with the 'Exception' tab selected. The left sidebar contains a menu with 'Media', 'Network', 'Storage', 'Event', 'VMS Edge', and 'System'. The main content area has tabs for 'Audio Alarm', 'External Input', 'External Output', and 'Exception'. Under 'Exception', there is a dropdown for 'Alarm Type' set to 'Network Disconnected', an 'Enable' checkbox that is checked, and an 'Alarm Action' section with checkboxes for 'External Output1' and 'Play Audio'. A 'Save' button is at the bottom.

Table 17. Description of the buttons

Parameters	Function Introduction
Alarm Type	Network Disconnected, IP Address Conflicted, SSD/HDD/RAID Full, SSD/HDD/RAID Uninitialized, SSD/HDD/RAID Error, No SSD/HDD/RAID and Low Voltage are available. Check the checkbox to enable the alarm type you selected.
Alarm Action	Refer to Table 13 (page 33) for the meanings of the items, here will not repeat again.

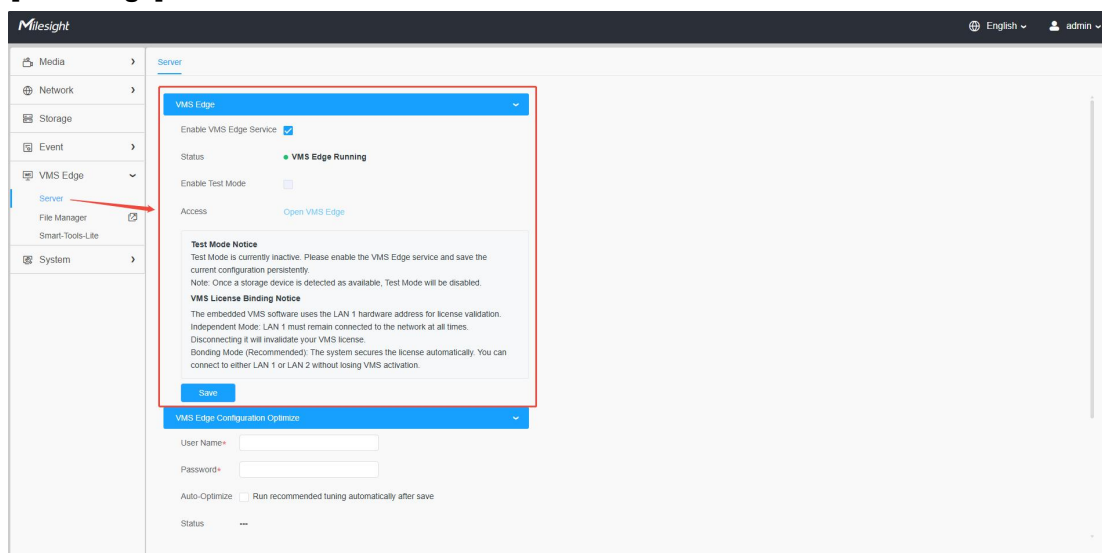
6.6 VMS Edge

The screenshot shows the Milesight web interface with the 'VMS Edge' configuration page. The left sidebar has 'VMS Edge' selected, with sub-items 'Server', 'File Manager', and 'Smart-Tools-Lite'. The main content area has a 'VMS Edge' dropdown menu. Below it, there is a section for 'VMS Edge Service' with an 'Enable VMS Edge Service' checkbox checked, a 'Status' indicator showing 'VMS Edge Running', an 'Enable Test Mode' checkbox, and an 'Access' link 'Open VMS Edge'. A 'Test Mode Notice' box contains text about test mode and license binding. Below this is a 'VMS License Binding Notice' box. At the bottom, there is a 'VMS Edge Configuration Optimizer' section with fields for 'User Name' and 'Password', an 'Auto-Optimize' checkbox, and a 'Status' indicator. A 'Save' button is also present.

VMS Edge is an auxiliary configuration and optimization tool for Nx Witness Server, specifically designed for Nx Witness Server series devices. Through the web management interface, users can flexibly connect to the Nx Witness Server and optimize its performance, assisting Nx Witness Server to operate more efficiently and reliably.

6.6.1 Server

[VMS Edge]



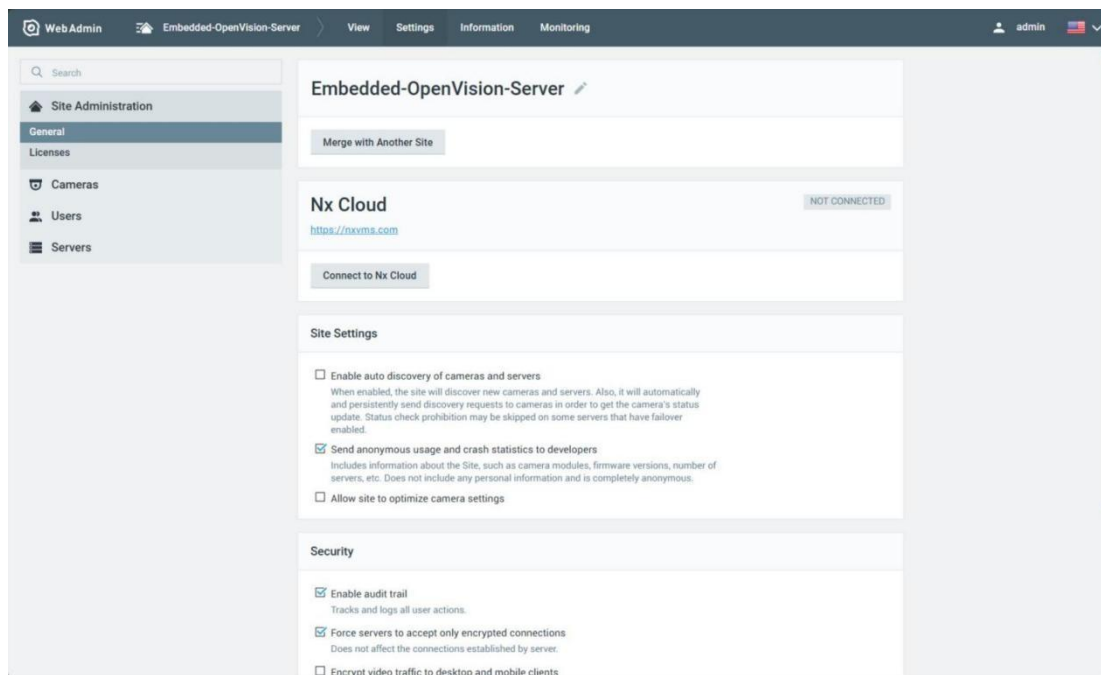
Step 1: Enable VMS Edge and verify whether the status shows "VMS Edge Running" first.

Step 2: Click [Open VMS Edge](#) to access the Nx Witness Server web page.

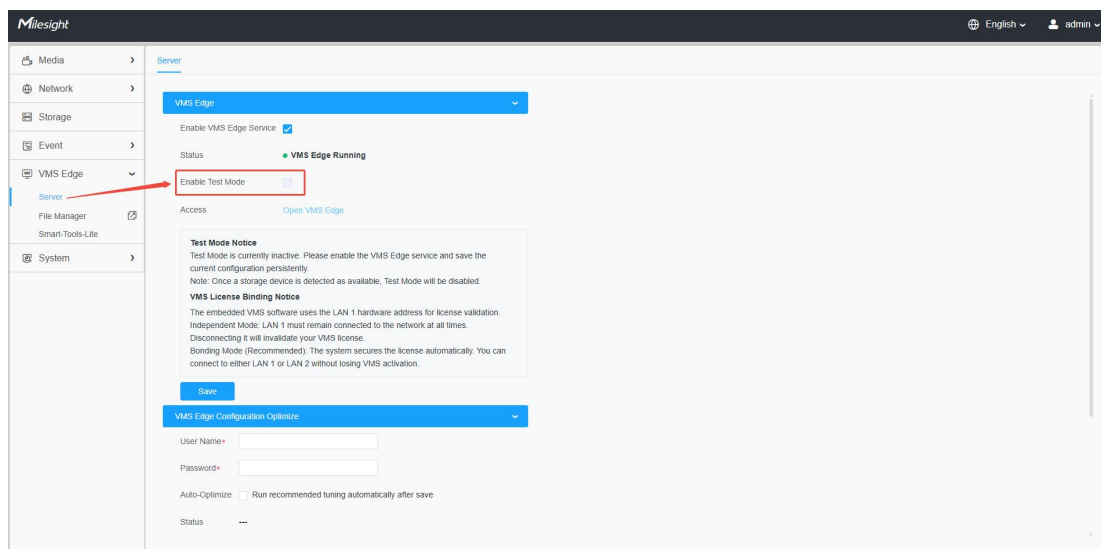
For first-time use, please click "Setup New System" to create a new system and complete the initialization. If a system has already been created, you can also choose to join an existing system.



After activation, you can access the Web Admin to configure Nx Witness Server and manage the system. The Nx Witness Server web interface supports Live View, device and user management, basic server settings, alarm and health status monitoring, enabling users to efficiently and conveniently manage the system.



[Test Mode]



Test Mode allows you to verify the Nx Witness Server configuration on a temporary basis without affecting the production system. When Test Mode is enabled, all configuration changes (including Save and Optimize operations) are treated as temporary and only take effect within the current boot cycle. This allows you to validate settings, camera connections, and storage configurations before deciding whether to make them permanent.

Enable Test Mode: Toggle the Test Mode switch to activate the testing environment. Note: Test Mode is only available when no HDD/SSD is inserted or the VMS Edge service is not running. Once an SSD/HDD is inserted and the system is operational, the Test Mode option will be grayed out.

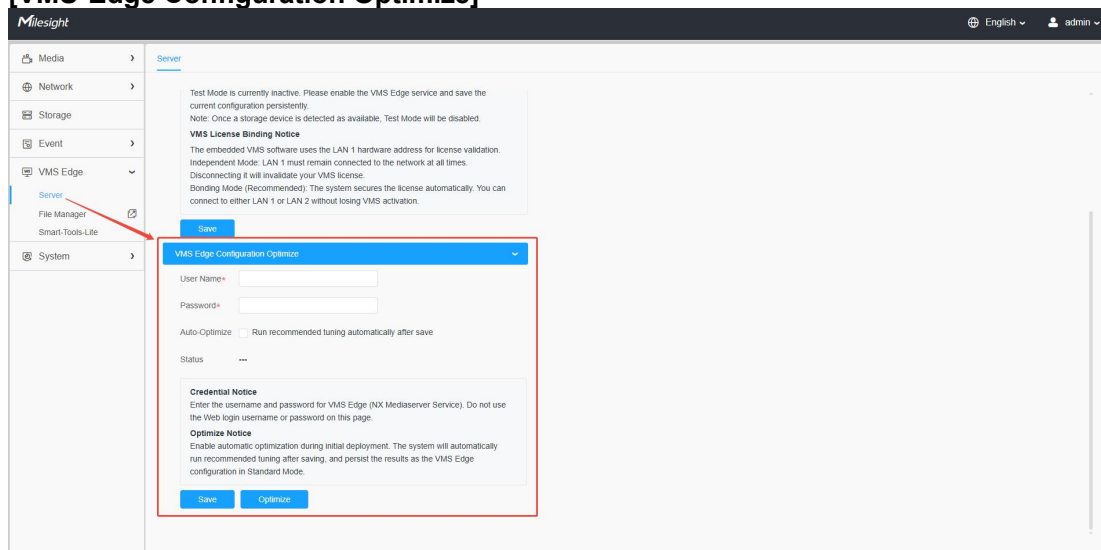
Temporary Configuration: While Test Mode is active, any configuration changes you make—including Save and Optimize operations—generate temporary configurations only. These temporary configurations take effect immediately for testing purposes but do not modify the permanent configuration.

Test Results: The system displays real-time test results including camera connectivity status, storage write speed, and system resource utilization.

Configuration Persistence: To make the tested configuration permanent, you must enable the VMS Edge service and use the standard Save function. There is no separate "Apply" button in Test Mode. All temporary configurations are automatically discarded when the device restarts, and the system reverts to the last permanently saved configuration.

Disable Test Mode: When you disable Test Mode, the temporary instance is removed. However, please note that temporary configurations are also discarded upon device restart regardless of whether Test Mode is manually disabled.

[VMS Edge Configuration Optimize]



This step primarily optimizes SSD storage for optimal performance. Please ensure it is enabled, as failure to do so may result in storage errors.

Step 1: Enable Auto-optimize.

Step 2: Enter the Nx Witness Server username and password, then click "Optimize". If the status displays "VMS Edge configuration was optimized", the optimization was successful.

 **Note:** Please make sure to enter the Nx Witness Server credentials, not those for the web interface.

6.6.2 File Manager

You can click File Manager in the sidebar to open a new window for file management, which supports the import and export of configurations, recordings, etc. This facilitates data backup for users and helps ensure data security.

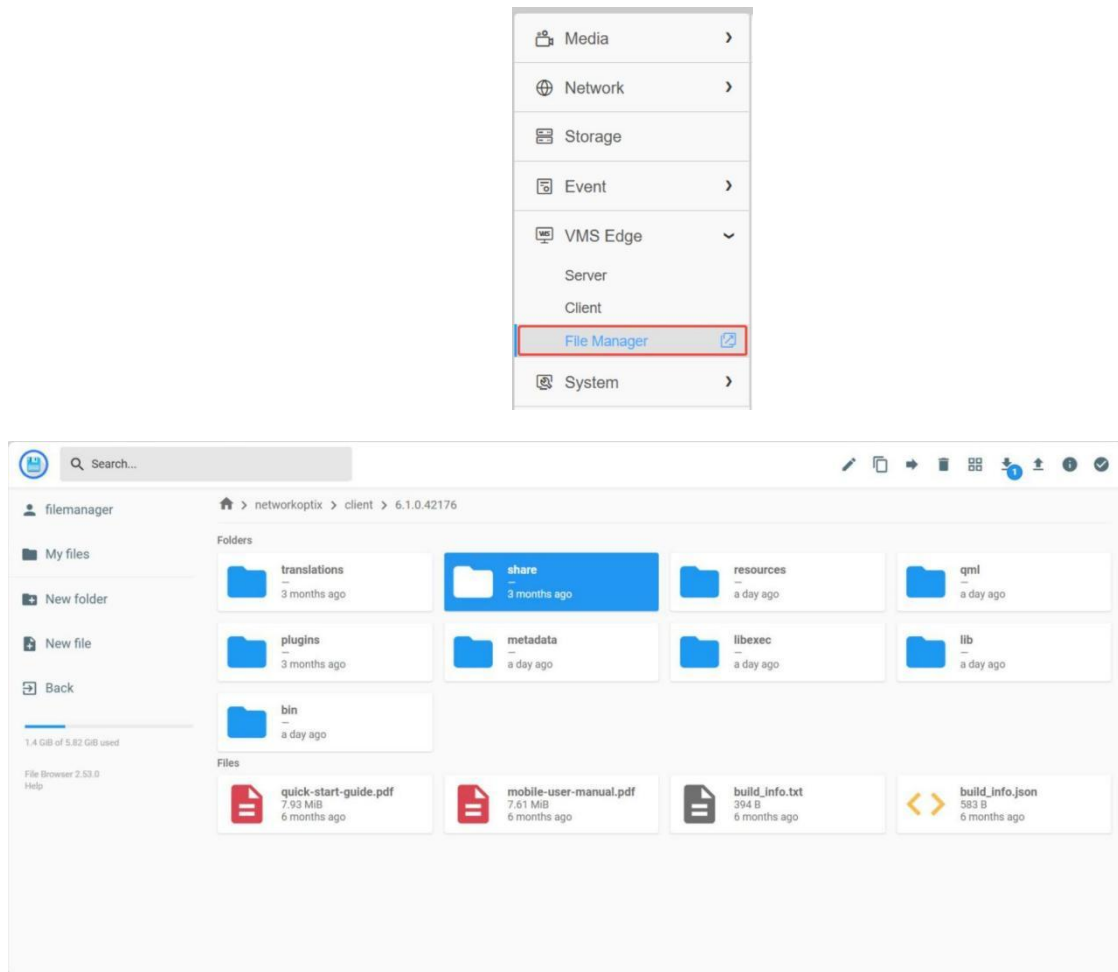


Table 18. Description of buttons

Parameters	Function Introduction
 Back	Click to return to the device web interface.
	Rename file.
	Copy file.
	Move file.
	Delete file.

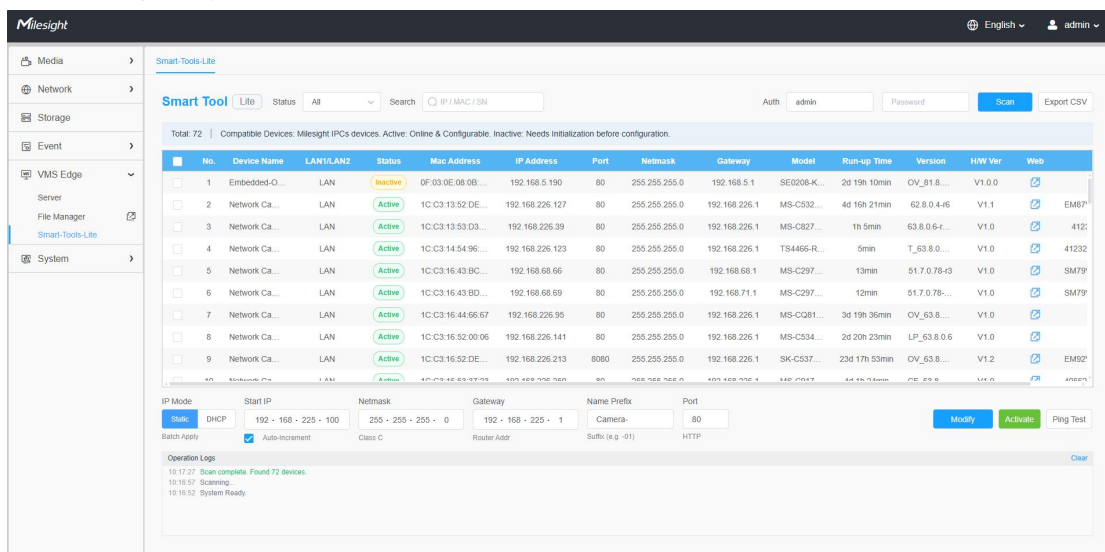
	Switch display mode.
	Download file.
	Upload file.
	File information, including Display Name and Last Modified Date.
	Enable multiple selection of files.

 **Note:** Do not modify or alter files in the "networkoptix" folder.

6.6.3 Smart Tools Lite

Smart Tools Lite is a built-in web-based utility that provides quick device discovery, batch configuration, and management tools for Milesight cameras directly from the OpenVision Server interface. No additional software installation is required.

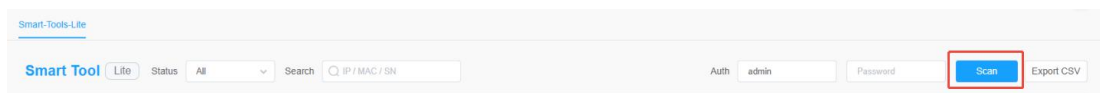
6.6.3.1 Page Layout



The Smart Tools Lite page consists of four main sections:

Section	Description
Header Toolbar	Global filters, search, authentication, and high-frequency actions
Device List	Table displaying discovered devices with status, network info, and selection
Config Dock	Batch configuration options and action buttons
Operation Logs	Real-time feedback for all operations

6.6.3.2 Device Discovery



Auto Scan:

Click "Scan" to discover compatible Milesight devices on the local network segment.

- A loading indicator displays during scanning
- Scan results refresh the device list in real-time
- The Total Count updates to show the number of discovered devices
- Scan completion is logged with the number of devices found

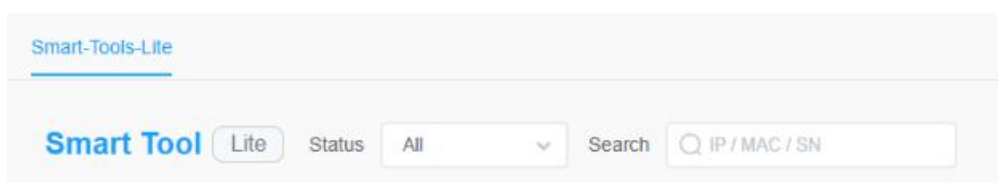
6.6.3.3 Device List

No.	Device Name	LAN1/LAN2	Status	Mac Address	IP Address	Port	Netmask	Gateway	Model	Run-up Time	Version	H/W Ver	Web
1	Embedded O...	LAN	Inactive	0F:03:0E:08:0B:...	192.168.5.190	80	255.255.255.0	192.168.5.1	SE0206-K...	2d 19h 10min	OV_81.8...	V1.0.0	
2	Network Ca...	LAN	Active	1C:C3:13:52:DE:...	192.168.226.127	80	255.255.255.0	192.168.226.1	MS-C532...	4d 16h 21min	62.8.0.4-r6	V1.1	EM87
3	Network Ca...	LAN	Active	1C:C3:13:53:D3:...	192.168.226.39	80	255.255.255.0	192.168.226.1	MS-C627...	1h 5min	63.8.0.6-r...	V1.0	412:
4	Network Ca...	LAN	Active	1C:C3:14:54:96:...	192.168.226.123	80	255.255.255.0	192.168.226.1	TS4466-R...	5min	T_63.8.0...	V1.0	41232
5	Network Ca...	LAN	Active	1C:C3:16:43:BC:...	192.168.68.66	80	255.255.255.0	192.168.68.1	MS-C297...	13min	51.7.0.78-r3	V1.0	SM79
6	Network Ca...	LAN	Active	1C:C3:16:43:BD:...	192.168.68.69	80	255.255.255.0	192.168.71.1	MS-C297...	12min	51.7.0.78...	V1.0	SM79
7	Network Ca...	LAN	Active	1C:C3:16:44:66:67	192.168.226.95	80	255.255.255.0	192.168.226.1	MS-CQ81...	3d 19h 36min	OV_63.8...	V1.0	
8	Network Ca...	LAN	Active	1C:C3:16:52:00:06	192.168.226.141	80	255.255.255.0	192.168.226.1	MS-C534...	2d 20h 23min	LP_63.8.0.6	V1.0	
9	Network Ca...	LAN	Active	1C:C3:16:52:DE:...	192.168.226.213	8080	255.255.255.0	192.168.226.1	SK-C537...	23d 17h 53min	OV_63.8...	V1.2	EM92

The device list displays the following columns:

Column	Description
No.	Sequential number
Device Name	Device identifier
LAN1/LAN2	Dual network port info
Status	Active (green badge) / Inactive (yellow badge)
MAC Address	Device MAC
IP Address	Current IP address
Port	HTTP port (default: 80)
Netmask	Subnet mask
Gateway	Default gateway
Model	Device model
Run-up Time	Device uptime
Version	Firmware version
H/W Ver	Hardware version
Web	Webpage jump icon. Click the Web icon to open the device's web interface in a new browser tab. Both Active and Inactive devices support this jump. The current Smart Tool Lite page remains open.
SN	Serial number

6.6.3.4 Filter and Search



- Status Filter: Select from All / Active / Inactive to filter devices by activation status.
- Keyword Search: Enter an IP address, MAC address, or SN to search for specific devices.

6.6.3.5 Global Authentication

Enter the default Username and Password for device operations.

Default Username: admin

Used for Scan, Batch Activate, and Batch Modify operations

If authentication fails, the failure reason is displayed in the Operation Logs

6.6.3.6 Batch IP Configuration

Batch IP Configuration allows you to modify network settings for multiple Active devices simultaneously.

Prerequisites:

- Only Active devices can be batch modified
- Maximum 16 devices per batch operation

Configuration Steps:

Step 1: Select target devices from the device list (checkbox selection or header select-all).

Step 2: In the Config Dock, configure the following parameters:

Parameter	Description
IP Mode	Static (manual configuration) or DHCP (auto-assigned)
Start IP	Starting IPv4 address for batch assignment (Static mode only)
Auto-Increment	When enabled, IPs increment sequentially from Start IP; when disabled, all devices use the same IP (conflict warning required)
Netmask	Subnet mask (Static mode only)
Gateway	Default gateway (Static mode only)
Name Prefix	Batch rename prefix (e.g., "Cam-" generates "Cam-01", "Cam-02"...); empty keeps original names
Port	HTTP port (default: 80)

Step 3: Click "Batch Modify" to apply configurations.

Rules and Validation:

- Static mode: Start IP, Netmask, and Gateway are required
- DHCP mode: Network parameter inputs are grayed out; Start IP, Netmask, and Gateway are not required
- IP address format validation is enforced
- Success/failure status is logged for each device
- Partial success returns: success count, failure count, skip count, and per-device results

6.6.3.7 Batch Activation

The screenshot shows the 'Smart Tool' interface. At the top, there's a search bar and a 'Scan' button. Below it, a table lists devices with columns: No., Device Name, LAN1/LAN2, Status, Mac Address, IP Address, Port, Netmask, Gateway, Model, Run-up Time, Version, HW Ver, and Web. A red box highlights the first 9 rows of the table, which are all marked as 'Inactive'. Below the table, there's a 'Batch Activation' dialog. It has fields for 'Start IP', 'Netmask', 'Gateway', 'Name Prefix', and 'Port'. The 'Start IP' is set to '192.168.225.100', 'Netmask' to '255.255.255.0', and 'Gateway' to '192.168.225.1'. The 'Name Prefix' is 'Camera-' and 'Port' is '80'. There are 'Modify' and 'Activate' buttons. The 'Activate' button is highlighted with a red box.

Batch Activation allows you to activate multiple Inactive devices in one operation by setting an initialization password.

Prerequisites:

- Only Inactive devices can be batch activated
- Mixed selection (Active + Inactive): Active devices are automatically skipped with a skip count logged

Activation Steps:

- Step 1: Select Inactive devices from the device list.
- Step 2: Click "Activate" to open the Batch Activate dialog.
- Step 3: Enter and confirm the new password:

New Password: 8-32 characters, must contain at least one number and one letter

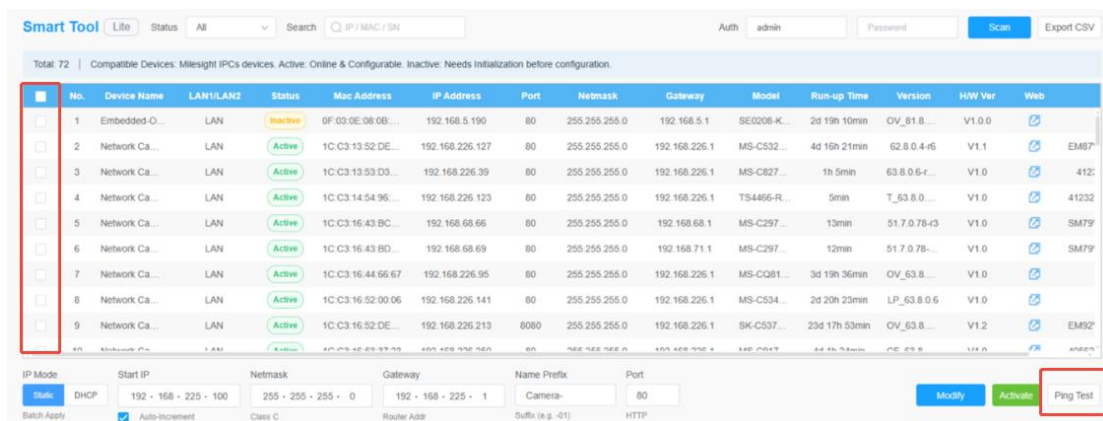
Confirm: Must match New Password exactly

- Step 4: Click "Confirm" to submit.

Results:

- Activation progress is displayed for each device
- Partial success returns: success count, failure count, skip count, and per-device results
- Device status updates to Active upon success
- Failed devices are listed with error reasons

6.6.3.8 Ping Test



Ping Test checks network connectivity for selected devices.

Steps:

Step 1: Select devices from the device list.

Step 2: Click "Ping" in the Config Dock.

Step 3: View results in the Operation Logs.

Results:

Per-device connectivity status is returned

Summary shows: selected count, reachable count, average latency

Results are logged with timestamps

6.6.3.9 Export CSV



Export the current device list as a CSV file.

Steps:

Step 1: Apply desired Status filter and/or Search to refine the list.

Step 2: Click "Export" in the Header Toolbar.

Step 3: The CSV file downloads with current filtered results.

6.6.3.10 Operation Logs



The Operation Logs panel displays real-time feedback for all page operations.

Log Levels:

Level	Color	Description
Info	Gray	General information (e.g., "System Ready", scan completion)
Success	Green	Successful operations
Error	Red	Failed operations with error reasons

Log Content:

- Timestamp
- Action type (Scan, Batch Modify, Batch Activate, Ping, Export)
- Target devices

- Result summary (success/failure/skip counts)
- Failure reasons for failed devices

Clear Logs: Click "Clear" to empty the current log display. This only clears the frontend display and does not affect backend audit logs.

Note: New logs append to the top of the panel. The log panel displays current session content only and does not persist across page refreshes.

6.7 System

Here you can configure System Setting, Security, Logs and Maintenance.

6.7.1 System Setting

Here you can check System information and Date&Time.

6.7.1.1 System Info

All information about the hardware and software of the device can be checked on this page.

Parameters	Value
Device Name	Embedded-OpenVision-Server
Product Model	SE0208-K/NX
Hardware Version	V1.0.1
Software Version	OV_81.8.0.4-r3-NX
System Version	OVSystem_81.8.0.4-r3
MCU Version	V2.0.26010501
BIOS Version	MTWL0403.V01
MAC Address	40:62:31:3B:7B:65
S/N	42150B034D099020
Device Information	KN1P0E03Y0N000000001P
Alarm Input	4
Alarm Output	2

Table 19. Description of the buttons

Parameters	Function Introduction
Device Name	The device name can be customized.
Product Model	The product model of the device.
Hardware Version	The hardware version of the device.

Software Version	The current software version of the device.
System Version	The current system version of the device.
MCU Version	The firmware version of the chip that controls basic hardware functions.
BIOS Version	The version of the low-level firmware that initializes hardware during startup.
MAC Address	Media Access Control address.
S/N	Serial Number of the device.
Device Information	The device information, including information about alarm I/O and clipper chip.
Alarm Input	The number of Alarm Input interface.  Note: The Alarm Input will appear only when the device have alarm input/output interface.
Alarm Output	The number of Alarm Output interface.  Note: The Alarm Output will appear only when the device have alarm input/ output interface.
Uptime	The elapsed time since the last restarted of the device.
	Save the configuration.

6.7.1.2 Date&Time

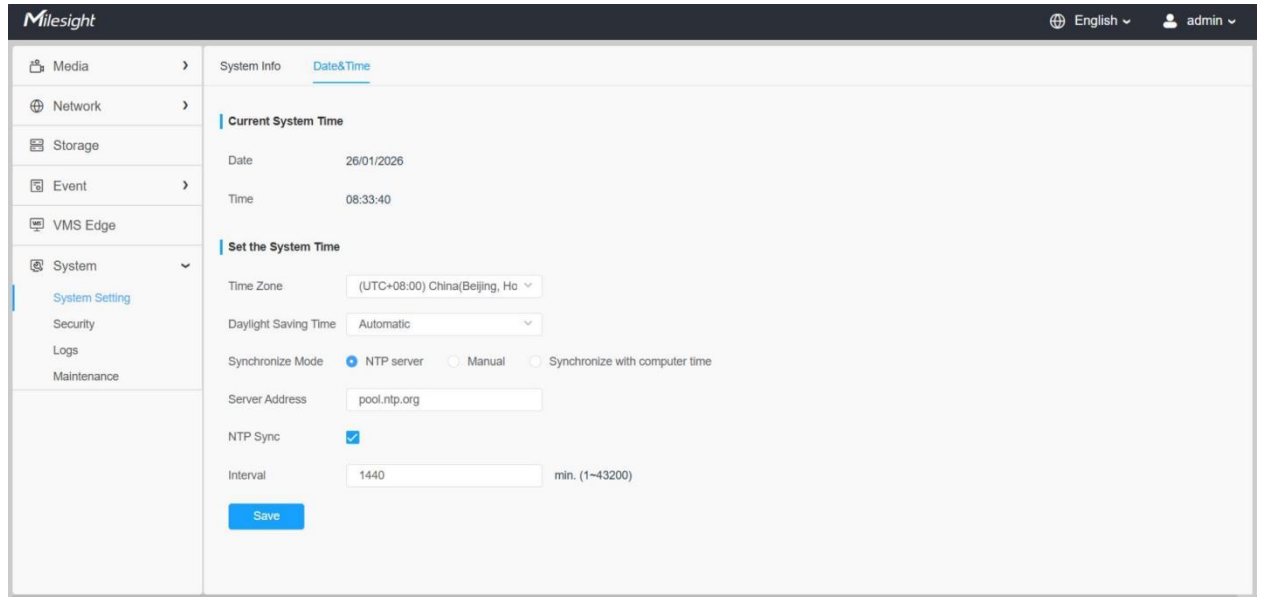


Table 20. Description of the buttons

Parameters	Function Introduction
Current System Time	Current date&time of the system.

Set the System Time	Time Zone: Choose a time zone for your location.
	Daylight Saving time: Enable the daylight saving time.
Set the System Time	Synchronize Mode: NTP server, Manual and Synchronize with computer time are optional. NTP server: Input the address of NTP server. NTP Sync: Regularly update your time according to the interval time. Manual: Set the system time manually. Synchronize with computer time: Synchronize the time with your computer.
Save	Save the configuration.

6.7.2 Security

Here you can configure User, Online User, Access List, Security Service, and About.

6.7.2.1 User

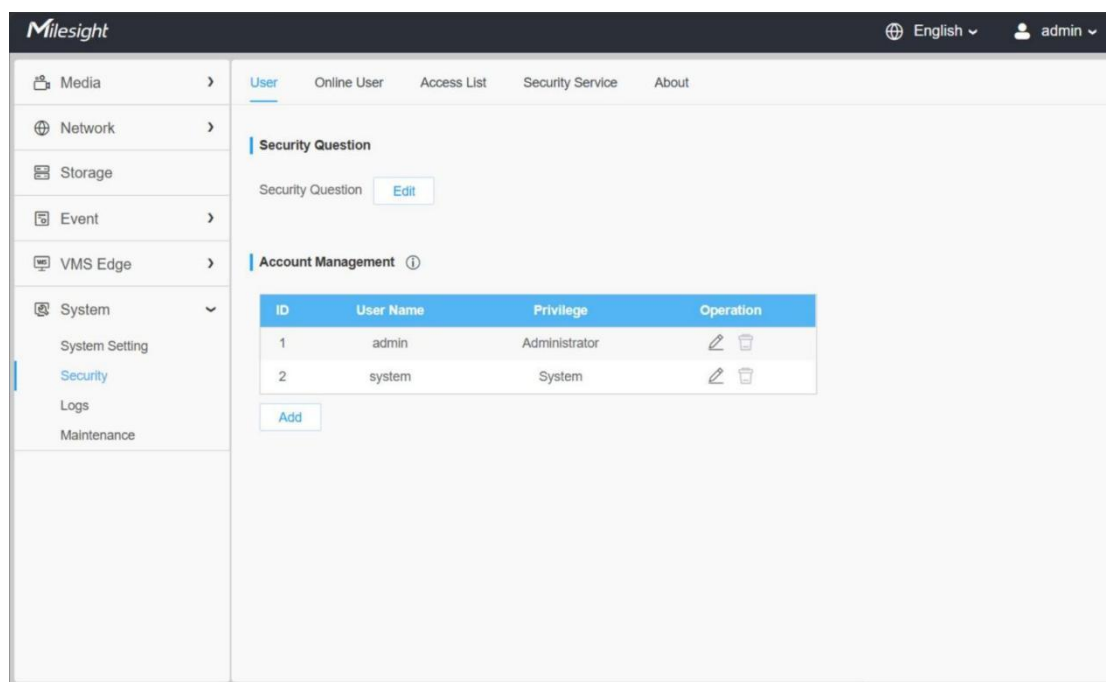
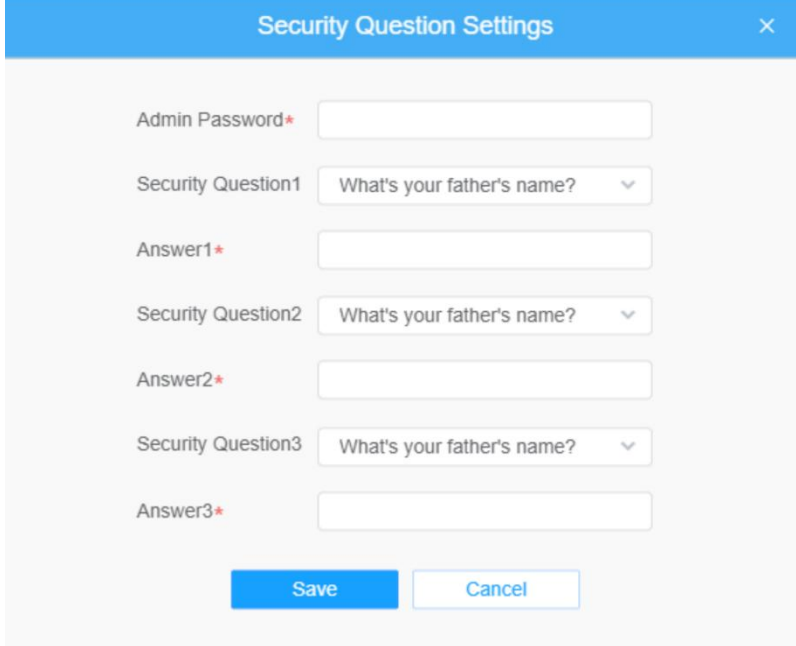
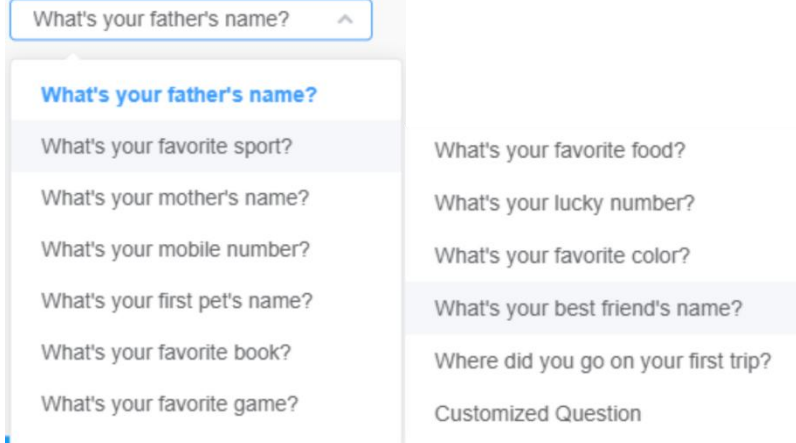
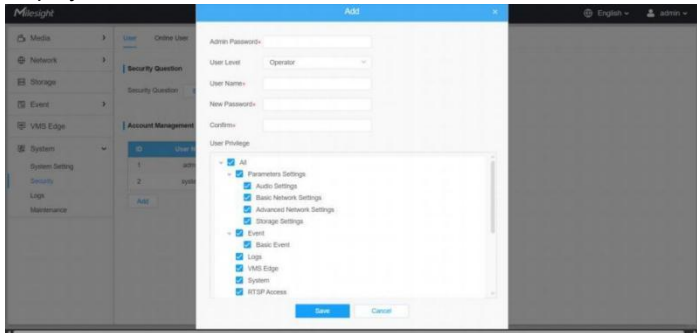


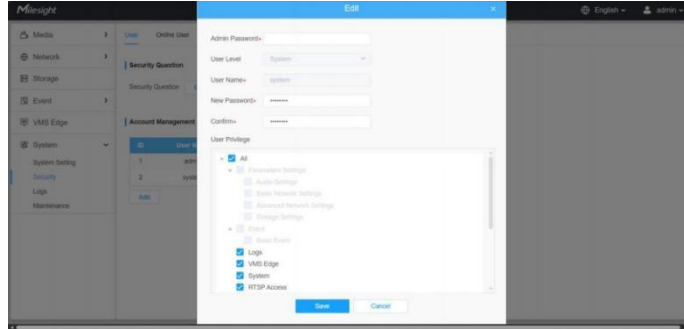
Table 21. Description of the buttons

Parameters	Function Introduction
Security Question	Click "Edit" button to set three security questions for your device. In case that you forget the password, you can click "Forget Password" button on login page to reset the password by answering three security questions correctly.

	 There are twelve default questions below, you can also customize the security questions. 
Parameters	Function Introduction
Account Management	Click “Add” button, it will display Account Management page. You can add an account to the camera by entering Admin Password, User Level, User Name, New Password, Confirm, and edit user privilege by clicking . The added account will be displayed in the account list.  Admin Password: You can add an account only after you enter the correct admin password. User Level: Set the privilege for the account. User Name: Input user name for creating an account.

New Password: Input password for the account.
 Confirm: Confirm the password.
 You can edit and delete the account in the account list under the admin account.
 For the default admin account, you can only change the password, and it cannot be deleted.

By clicking , you can edit the detailed information of a custom user, including user level, name, password, privileges, and more.



Note:

- Support up to 20 users, including a default user and 19 custom added users.
- The operator privilege is all checked by default.

6.7.2.2 Online User

Here real-time status of user logging in the device will be shown.

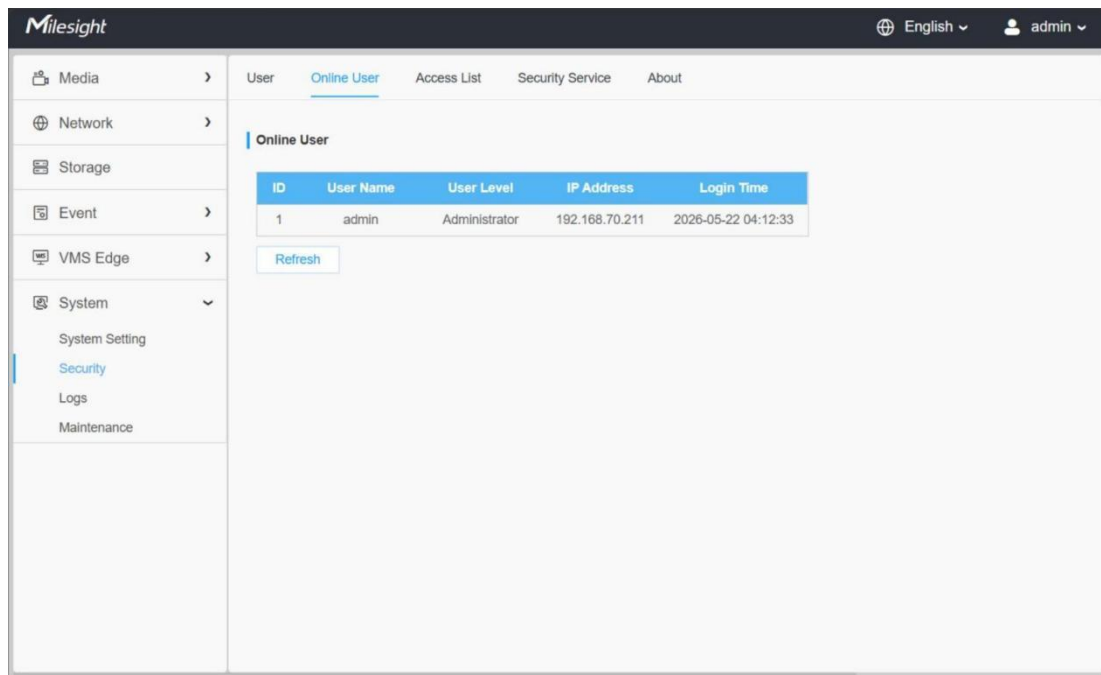


Table 22. Description of the buttons

Parameters	Function Introduction
Refresh	Click to get latest status of user accessing to the device.

ID	Record serial number of user logging in the device.  Note: • There are at most 30 records shown at the list. • There is only one record if the same user logging on camera by the same IP address.
User Name	Name of user logging in the device.
User Level	Level of user logging in the device.
IP Address	Device IP address where user logging in the device web located.
Login Time	System time of user logging in the device.

6.7.2.3 Access List

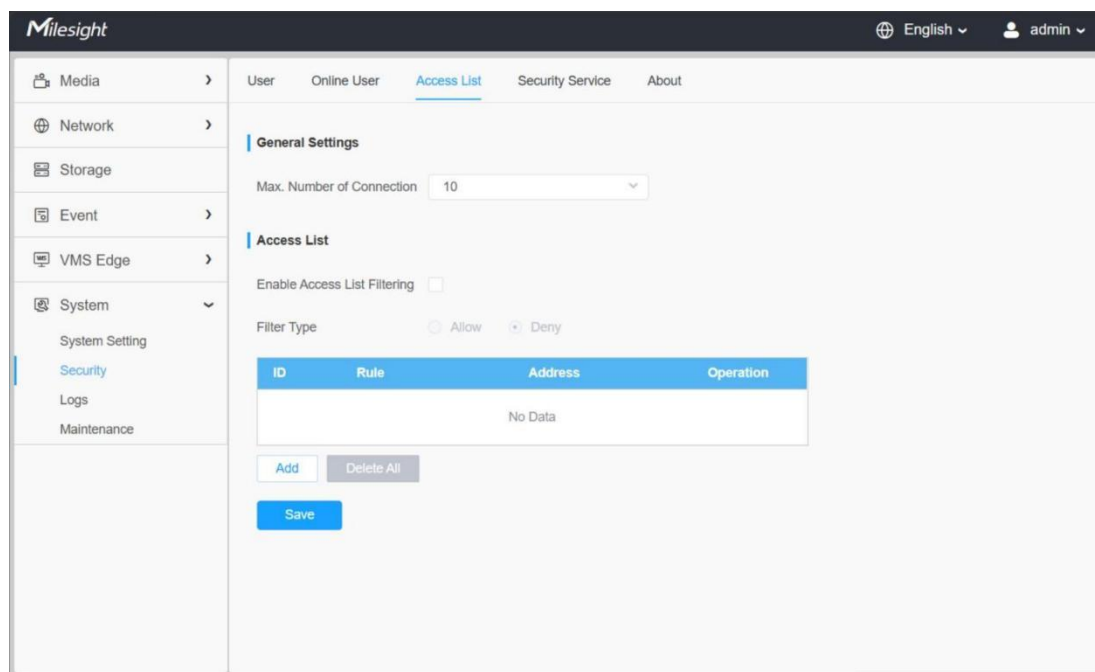
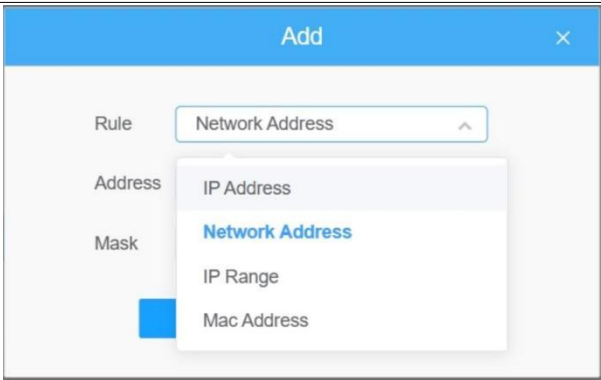
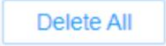
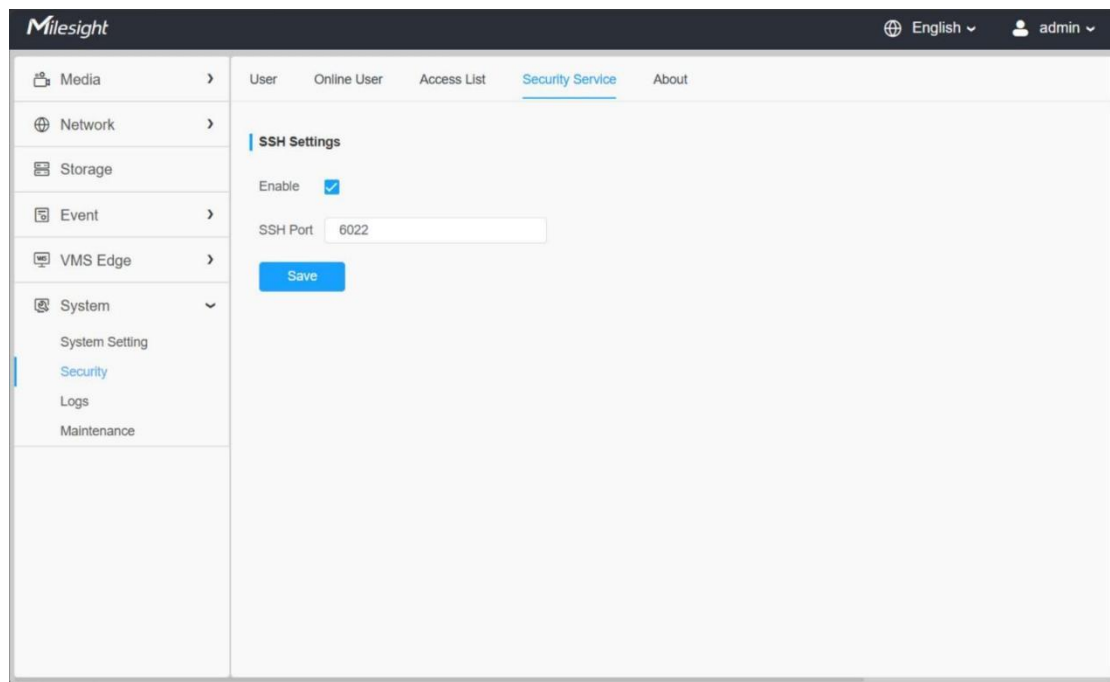


Table 23. Description of the buttons

Parameters	Function Introduction
General Settings	Max. Number of Connection: Select the maximum number of concurrent streaming. Options include No Limit, 1~10.
Access List	Enable Access List Filtering: Able to access or restrict access for some IP address.
	Filter type: Allow or deny access.
Parameters	Function Introduction

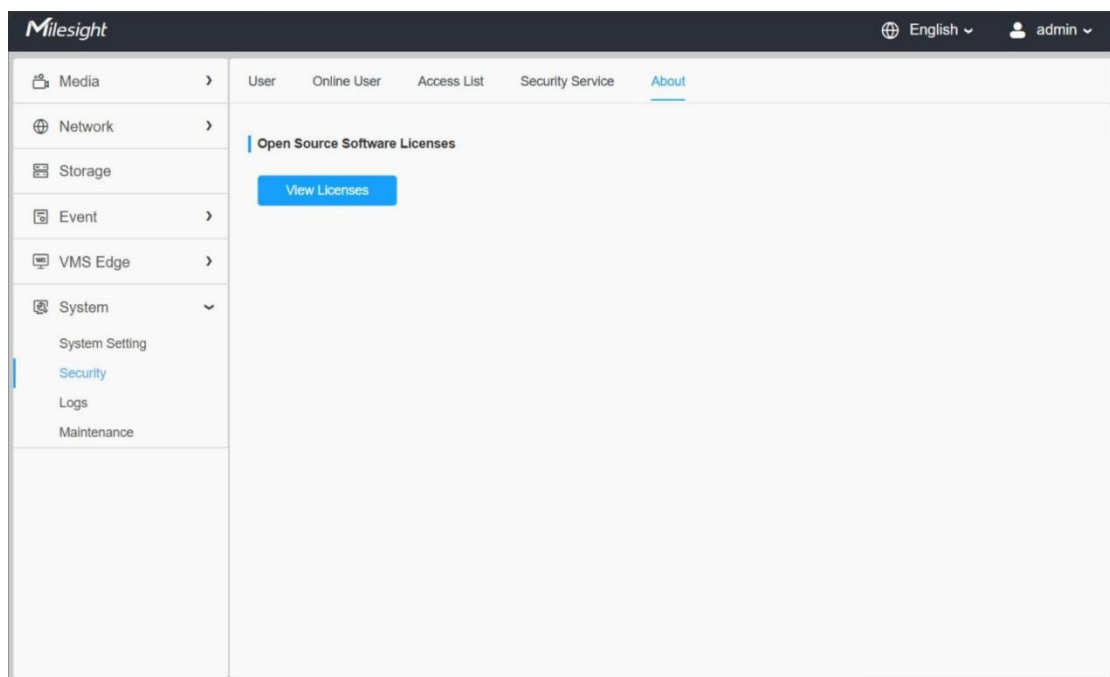
Access List		 Rule: IP Address, Network Address, IP Range and Mac Address are available. IP address: Input the IP address to get the access to the device. Network Address: Input the network address to gain access to the device. You also need to set the mask value to complete the addition. IPv4: Valid mask range is 0~32 IPv6: Valid mask range is 0~128 IP Range: Input the IP address to get the access to the device. Mac Address: Input the Mac address to get the access to the device.
		Delete all the access list.
		Edit the selected IP on access list.
		Delete the selected IP on access list.
		Save the configuration.

6.7.2.4 Security Service

**Table 24. Description of the buttons**

Parameters	Function Introduction
SSH Settings	Secure Shell (SSH) has many functions: it can replace Telnet and also provides a secure channel for FTP, POP, even for PPP.  Note: Enabling this feature may pose security risks. It is recommended to keep it disabled.

6.7.2.5 About



User can view some open source software licenses about the device by clicking the View Licenses button.

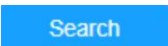
6.7.3 Logs

The section describes the information about **Security Audit Logs**, and **Remote Logs**.

6.7.3.1 Security Audit Logs

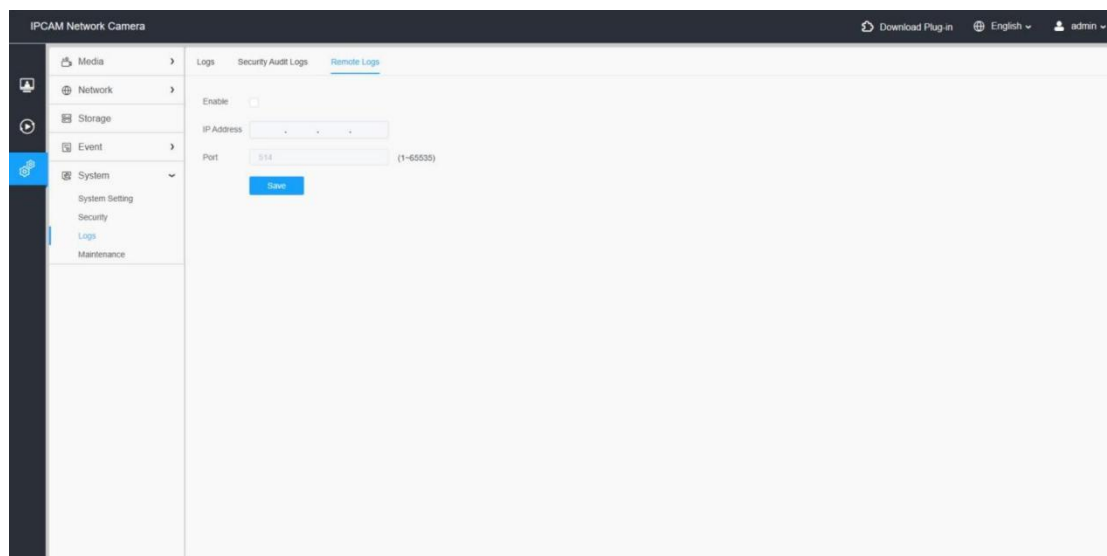
Time	Main Type	Sub Type	Param	User	IP	Detail
2026-01-26 08:31:00	Operation	RTSP Session Stop	-	admin	192.168.77.170	-
2026-01-26 08:31:00	Operation	Logout Remotely	-	admin	192.168.77.170	-
2026-01-26 08:30:41	Operation	RTSP Session Start	-	admin	192.168.77.170	-
2026-01-26 08:30:41	Operation	Login Remotely	-	admin	192.168.77.170	-
2026-01-26 08:29:26	Operation	Login Remotely	-	admin	192.168.70.211	-
2026-01-26 07:30:43	Operation	RTSP Session Stop	-	admin	192.168.77.170	-
2026-01-26 07:30:43	Operation	Logout Remotely	-	admin	192.168.77.170	-
2026-01-26 07:30:23	Operation	RTSP Session Start	-	admin	192.168.77.170	-
2026-01-26 07:30:23	Operation	Login Remotely	-	admin	192.168.77.170	-
2026-01-26 06:30:24	Operation	RTSP Session Stop	-	admin	192.168.77.170	-
2026-01-26 06:30:24	Operation	Logout Remotely	-	admin	192.168.77.170	-

Table 25. Description of the buttons

Parameters	Function Introduction
Main Type	There are five main log types: All Type, Event, Operation, Information and Exception.
Sub Type	On the premise that main type has been selected, select the sub type to narrow the range of logs.
Start Time	The time log starts.
End Time	The time log ends.
	Search the logs.
	Export the logs.
Go to	Input the number of logs' page.

6.7.3.2 Remote Logs

This section is about how to forward logs to a third-party server for centralized management.



Step 1: Enable Log Forwarding Turn on the Enable option to activate log forwarding.

Step 2: Enter Destination IP Address In the IP Address field, enter the destination IP address of the server that can receive the logs.

Step 3: Specify Port Number In the Port field, specify the port number used by the receiving server to accept log data.

6.7.4 Maintenance

Here you can configure System Maintenance and Auto Reboot.

6.7.4.1 System Maintenance

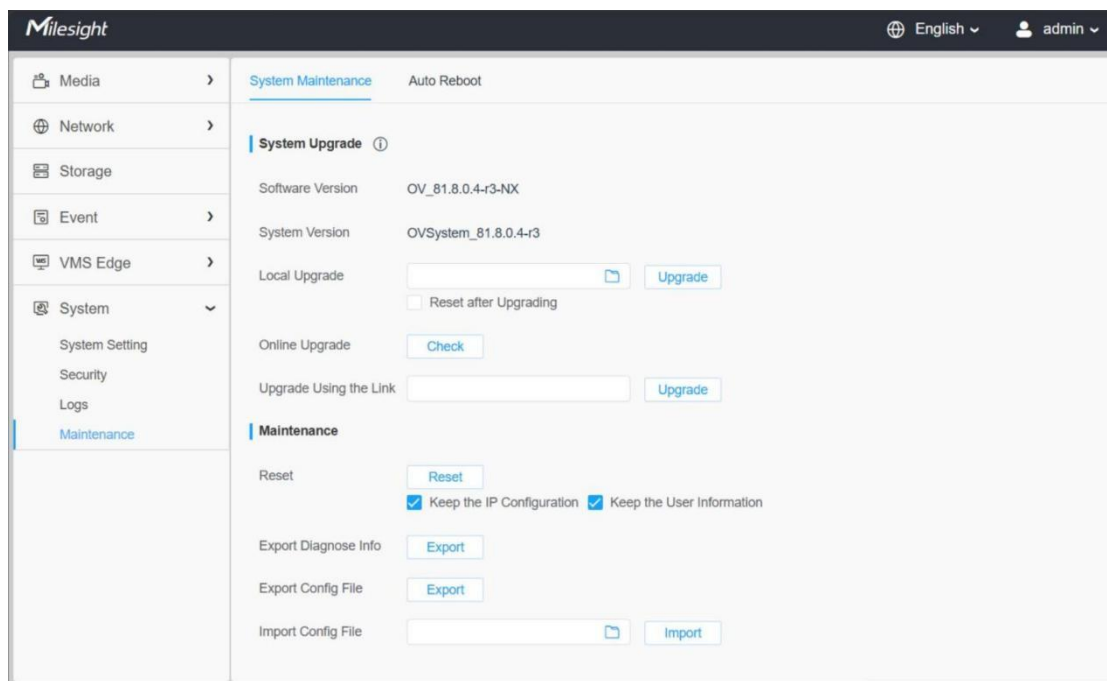
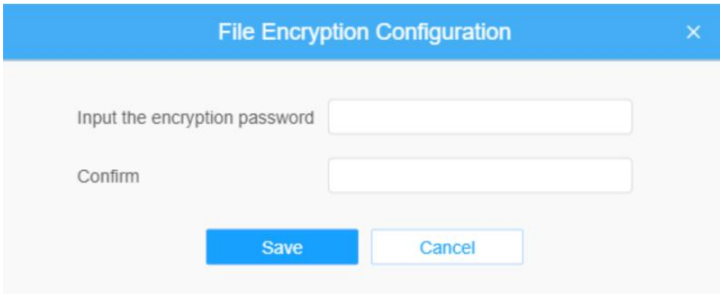
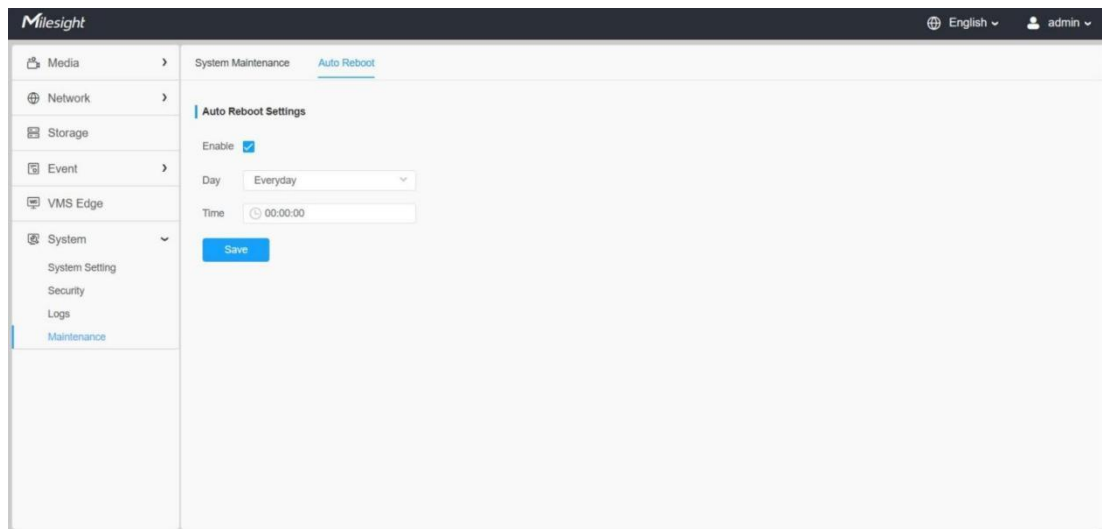


Table 26. Description of the buttons

Parameters	Function Introduction
System Upgrade	Software Version: The software version of the device. System Version: The system version of the device. Local Upgrade: Click the  button and select the upgrading file, then click the "Upgrade" button to upgrade. After the system reboots successfully, the update is done. You can check "Reset after Upgrading" to reset the device after upgrading it. Online Upgrade: Click the "Check" button to check the current latest software version and system version on our website, and then click "OK" to upgrade to the latest version. It will pop up the following prompt if your device is already the latest version.  Upgrade Using the Link: When you have uploaded the upgrading file to the cloud, like Google Driver, etc., you can input the link address and then click the "Upgrade" button to upgrade. Note: Do not disconnect the power of the device during the update. The device will be restarted to complete the upgrading.
Maintenance	Reset: Click "Reset" button to reset the device to factory default settings. Keep the IP Configuration: Check this option to keep the IP configuration when resetting the device. Keep the User information: Check this option to keep the user information when resetting the device. Export Diagnose Info: Click this button to export logs and system information of the device operation status. Note: The file format is ".txt". Export Config File: Click this button and a window will pop up as shown below:  You need to enter and confirm password again, then click save button to export configuration file. Import Config File: Click this button, then a window will pop up and you can click "OK" to update the configuration. It will pop up a window to prompt "Input the password of config file", then enter password and click save button to import configuration file.

	File Encryption Configuration Input the encryption password Save Cancel Note: Export and import the same configuration file. Password must be the same. Language File: Here, you can edit, export, and reset the language file. Import Language File: Import the language file then click the "Import" button, then a window will pop up and you can click "OK" to update the configuration. It allows you to modify or import predefined language translation packs, enabling you to customize the interface language based on your preferences, achieving better adaptation to various linguistic environments.
Reboot	Click "Reboot" button to restart the device immediately.

6.7.4.2 Auto Reboot



Set the date and time to enable Auto Reboot function, the device will reboot automatically according to the customized time in case that device overload after running a long time.

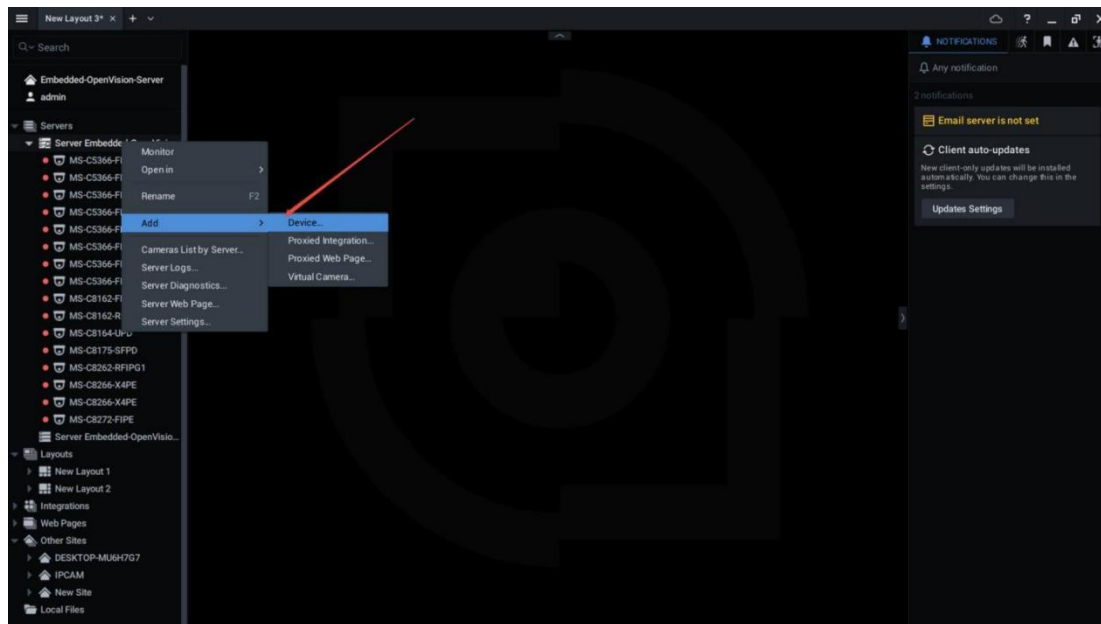
Chapter 7. Integration with Nx Witness Server

Users can directly open the Nx Witness Client on your PC or access via the web interface to perform subsequent compatibility-related configurations. For detailed instructions, refer to the previous chapter [6.6 VMS Edge](#).

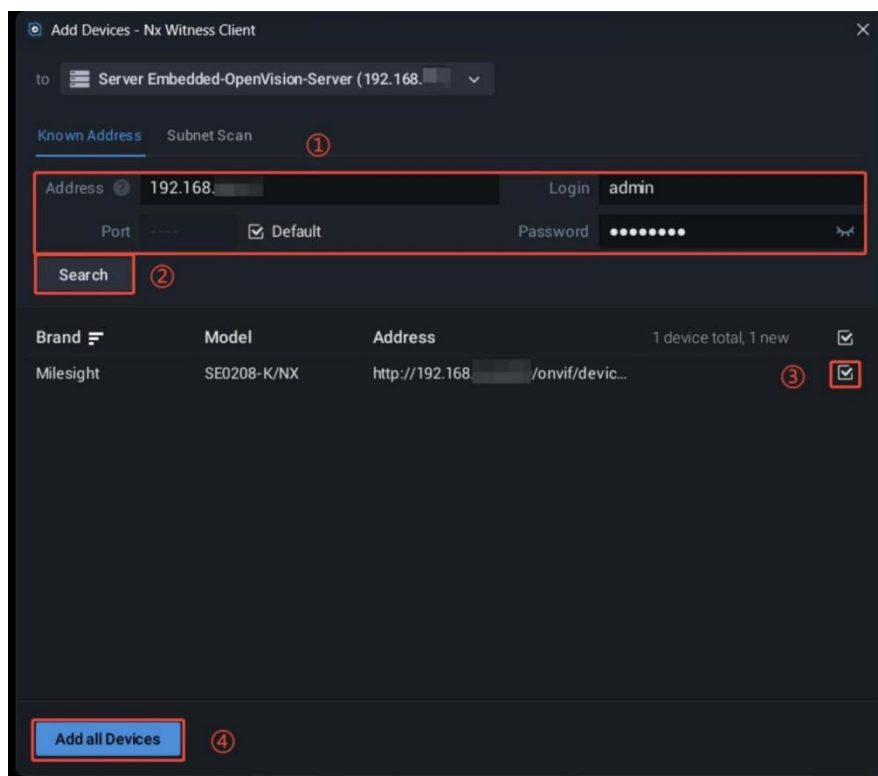
7.1 Add Device

Milesight OpenVision Server can be integrated into Nx Witness via ONVIF, enabling both alarm input and alarm output functions.

Step 1: Right-click the server, then select Add --> Device from the pop-up window.



Step 2: Enter the device's IP address, username, and password, then click "Search". Once the device is found, check the box next to it and click "Add all Device" to add it.

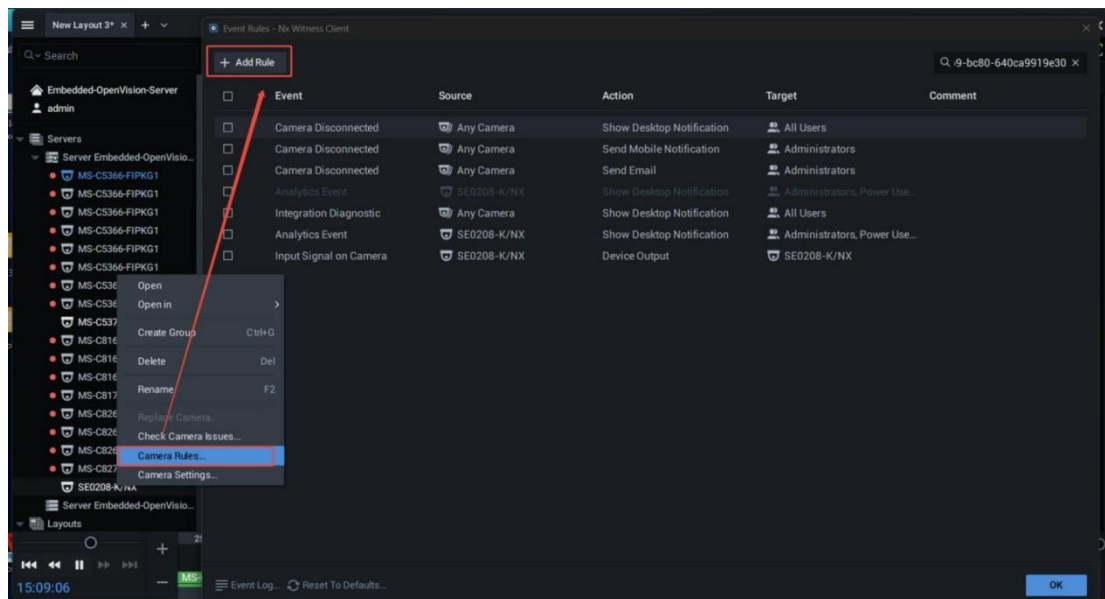


7.2 Alarm I/O

With seamless integration into the Nx Witness Client, users can receive and manage

external alarm input signals in real time, and also configure event-based actions to control external devices via alarm outputs directly from the client.

Step 1: Right-click the device and choose "Camera Rules". Then click "Add Rule" in the pop-up window.



Step 2: Select "Input Signal on Camera" in the pop-up window and complete the parameter configuration. There are two sections, "Event" and "Action" section.

- Event Section:

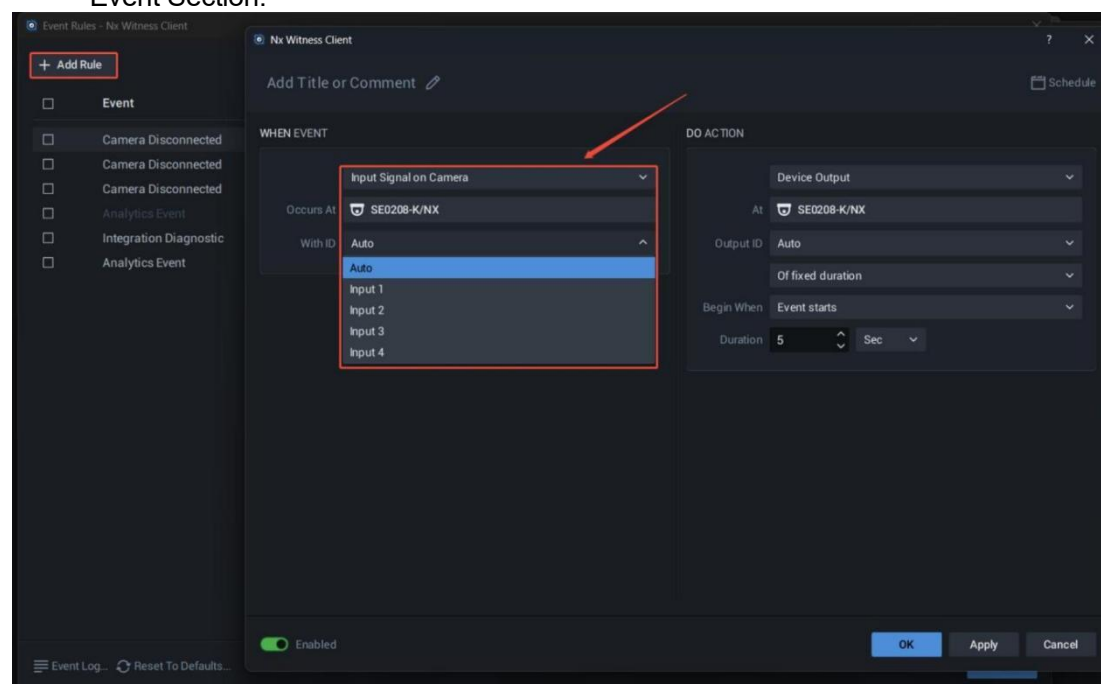


Table 27. Description of Fields

Parameters	Function Introduction
Occurs At	Click in this field to select devices to monitor, all devices can be selected.

With ID	Used to select the specific alarm input channel. Auto: The system automatically detects and handles all available alarm input ports. Input 1 / Input 2 / Input 3 / Input 4: These represent the 1st, 2nd, 3rd, and 4th alarm input ports on the device. Users can select the corresponding input port to trigger the event.
---------	---

• Action Section:

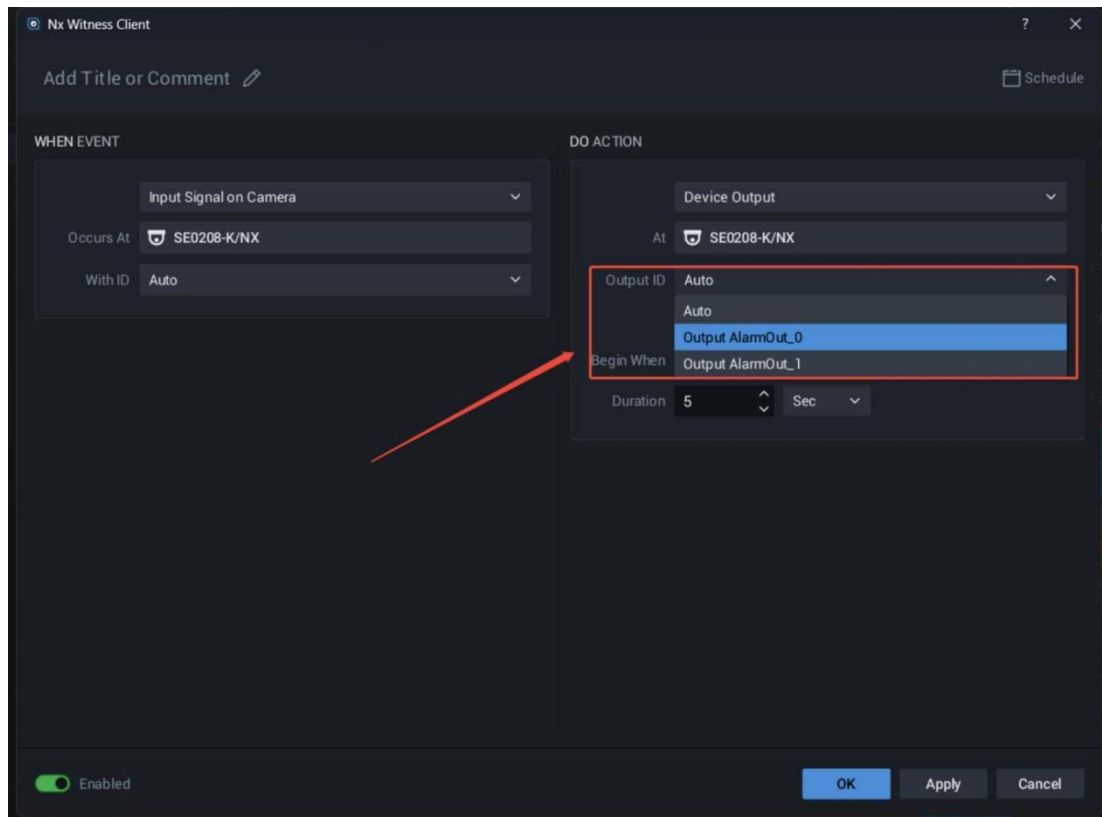
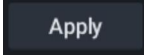
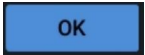


Table 28. Description of Fields

Parameters	Function Introduction
At	Click in this field to select devices to action, all devices can be selected.
Output ID	Used to select which alarm output port will be activated when the event is triggered. Auto: The system automatically selects the output port. Output AlarmOut_0 / Output AlarmOut_1: The alarm output ports on the device.

Of fixed duration	The action will be performed for a specified period of time. When this option is selected, the following fields will appear: - o Begin When: Defines when the action should start. ■ Event Starts: The action begins when the event is detected. ■ Event Stops: The action begins when the event ends. - o Duration: Sets the length of time (in seconds) the action remains active.
For the duration of even	The action will remain active for as long as the event is ongoing. When the event ends, the action will stop automatically.

Step 3: Then click  to save or click  to finish the configuration.

7.3 Audio Input

Step 1: Right-click the device and choose "Camera Rules". Then click "Add Rule" in the pop-up window.

Step 2: Select "Analytic Event" and in the pop-up window and complete the parameter configuration. There are two sections, "Event" and "Action" section.

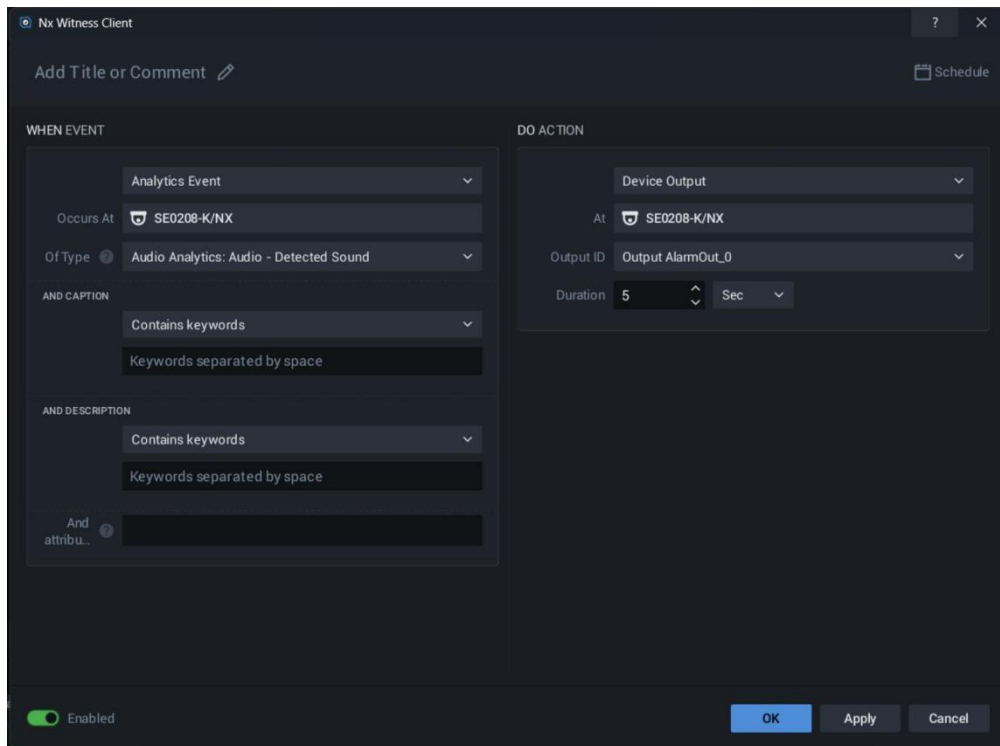
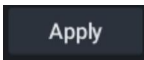
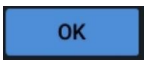


Table 29. Description of Event Fields

Parameters	Function Introduction
------------	-----------------------

Occurs At	Click in this field to select devices to monitor, all devices can be selected.
Of Type	Used to select the specific event type supported by the selected device.
AND CAPTION	Used to further filter events based on the caption (title or label) associated with the event. Multiple matching methods are provided: - Contain keywords: The event will be triggered if the caption contains the specified keywords. - not Contain keywords: The event will be triggered if the caption does not contain the specified keywords. - is listed: The event will be triggered only if the caption matches any item in the Allow List or Block List. - is not listed: The event will be triggered if the caption does not match any item in the Allow list or Block List.
AND DESCRIPTION	Used to filter events based on the event description. The matching methods are the same as for CAPTION. Here will not repeat again.
AND attribute	A text field where users can input specific attributes. The event will be triggered only if the event matches the specified attribute(s).

Step 3: Then click  to save or click  to finish the configuration.

7.4 Play Sound

Step 1: Right-click the device and choose "Camera Rules". Then click "Add Rule" in the pop-up window.

Step 2: Select "Analytic Event" and in the pop-up window and complete the parameter configuration. There are two sections, "Event" and "Action" section.

The screenshot shows the 'Nx Witness Client' interface for configuring an action. The 'DO ACTION' section is active, with 'Play Sound' selected in the dropdown menu. Below this, 'Alarm Clock 2' is chosen as the sound, with a 'Manage' button next to it. The action is configured to occur 'At' device 'SE0208-K/NX' and be sent 'To Users' 'Administrators'. A volume slider is present with a 'Test' button. The 'INTERVAL OF ACTION' is set to 'Once in 1 Min'. The 'WHEN EVENT' section on the left shows event details like 'Analytics Event', 'Occurs At', 'Of Type', and 'AND CAPTION'. At the bottom, there are 'OK', 'Apply', and 'Cancel' buttons, and a status indicator 'Enabled'.

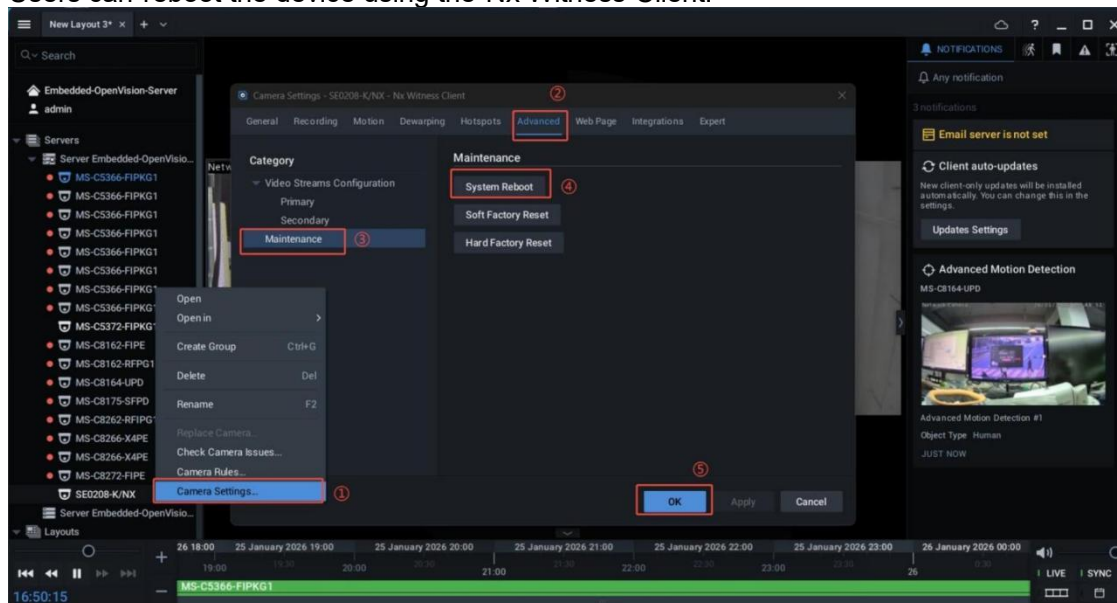
For details on the Event section fields, please refer to [Table 29](#). Here will not repeat again.

Table 30. Description of Action Fields

Parameters	Function Introduction
Sound	Select a sound to play when the event is triggered. Options include: No Sound, Alarm Clock 2, Alarm Clock 3, Bicycle Bell, Door Bell, Notification 1-3, Siren 1, Syren 1, etc. You can click Manage to play, add, rename, or delete sounds.
At	Select the device on which the sound will be played.
To Users	Select the users who will receive this action
Volume	Adjust the volume for the selected sound.
Interval of Action	Set the minimum interval between repeated actions

7.5 Reboot

Users can reboot the device using the Nx Witness Client.



Step 1: Right-click on the device and select "Camera Settings".

Step 2: Go to the "Advanced" tab.

Step 3: Click on "Maintenance".

Step 4: Choose "System Reboot" to initiate the reboot process.

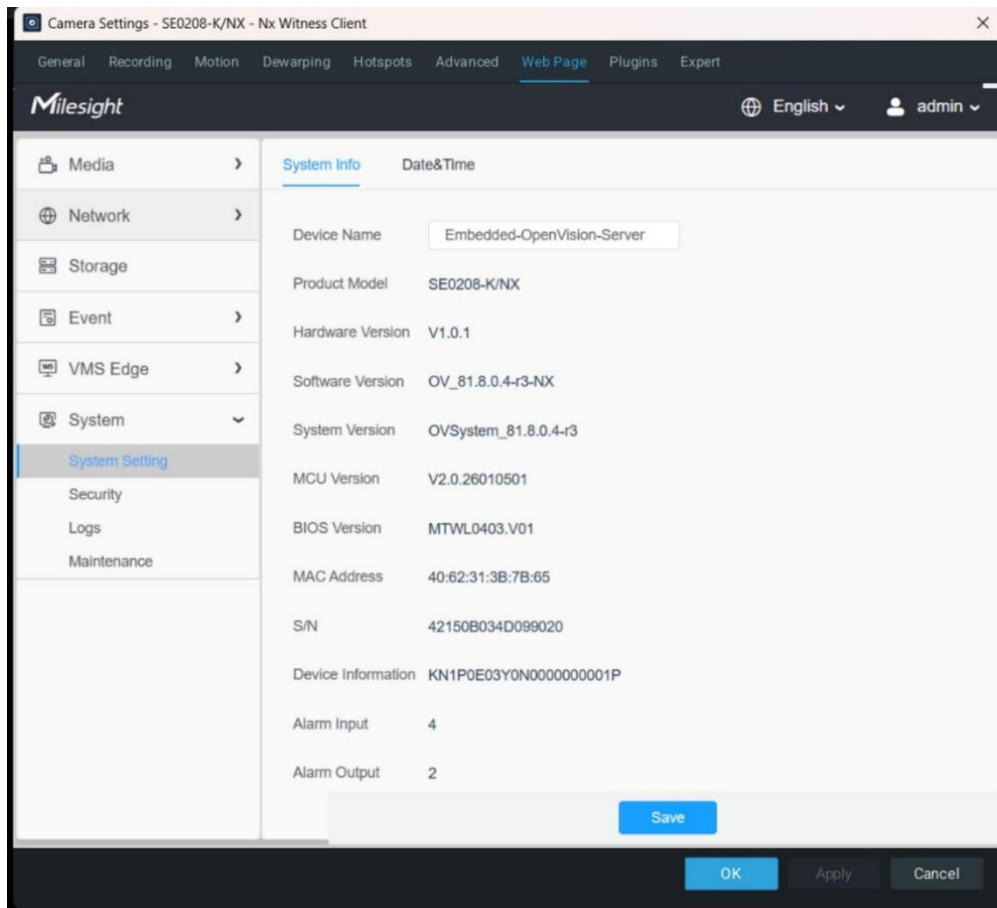
Step 5 : Click "OK".

7.6 Web Page

Users can also access the device's web interface through the Nx Witness Client.

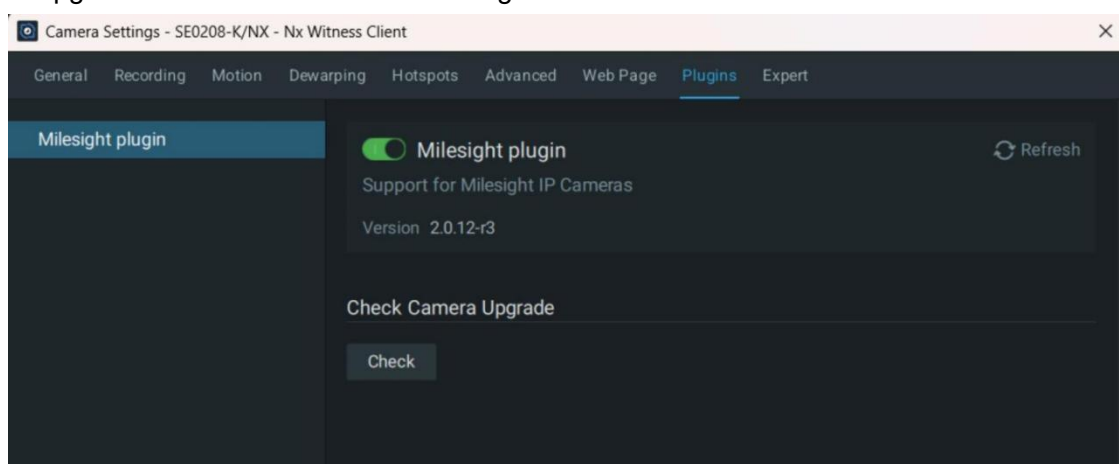
This feature allows users to directly open the device's built-in web page for advanced configuration, or accessing features not available in the Nx Witness Client. By accessing the web interface, users can manage firmware updates, network settings, user accounts, or other functions.

Steps: Right-click the device and select "Camera Settings" —>"Web Page".



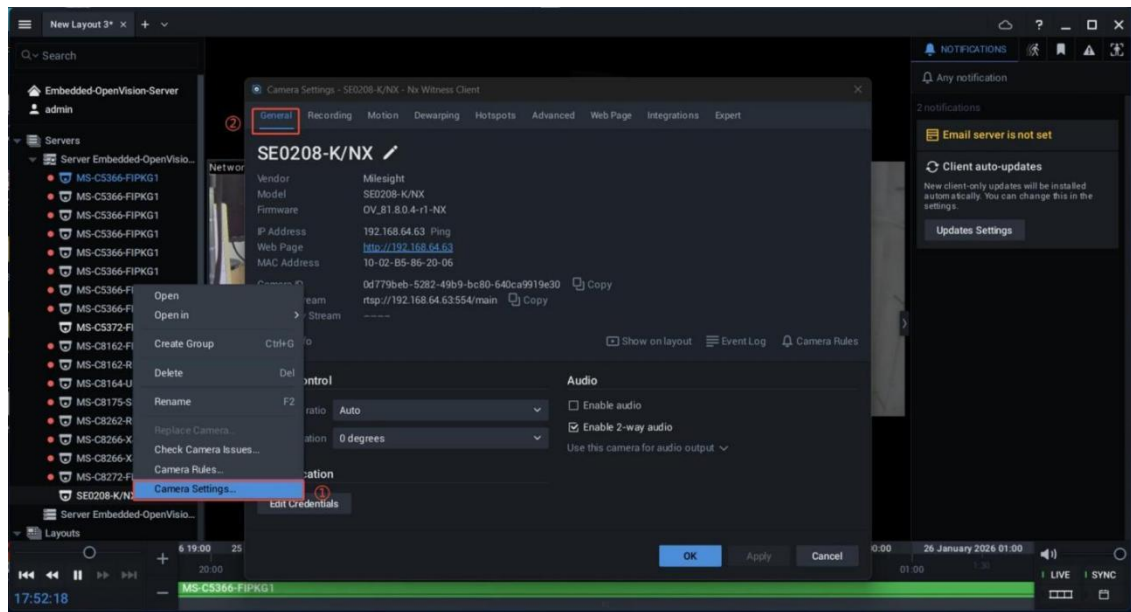
7.7 Firmware Upgrade

Milesight OpenVision Server is equipped with an integrated Nx Plugin, enabling users to upgrade device firmware online through the Client interface.

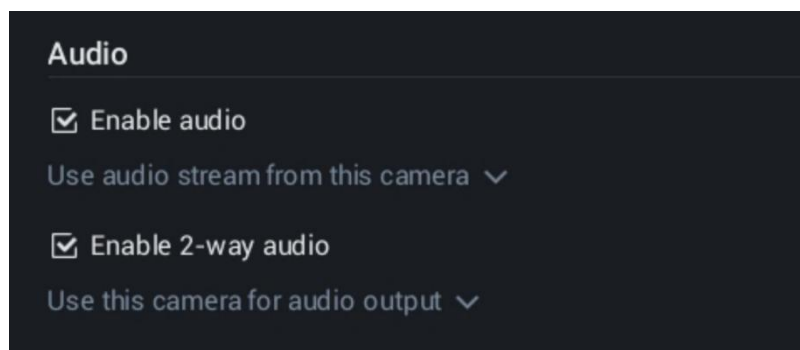


7.8 Device Info

Users can click Camera Setting --> General to view relevant device information, including Vendor, Model, Firmware, IP Address, and more.



[Audio]



In the audio settings section, there are two options: Enable Audio and Enable 2-way Audio. These settings define how the server manages audio streams for connected devices.

1. Enable audio

This option allows you to enable audio recording for the device. You can choose one of the following:

- Use audio stream from this camera: The system will record audio directly from the microphone built into this device.
- Use audio stream from another camera: The system will record audio from other camera's microphone. This is useful if you want to synchronize video from one camera with audio from another.

2. Enable 2-way Audio

This option allows for two-way communication through the device. You can select:

- Use this camera for audio output: The device will play audio received from the client (for example, you can speak through the client and your voice will be played through the speaker).

- Transmit audio stream to another camera: The audio received from the client will be sent to another camera for output. This is useful if you want to control which camera broadcasts your voice.

Chapter 8. FAQ

This chapter addresses frequently asked questions and common problems that users may face during the operation of the device. For each issue, possible causes and recommended solutions are provided. If your problem persists after following these steps, please contact our customer support for further assistance.

1. Pre-Deployment

Q: What SSD / HDD types, brands, and capacities are recommended?

A: Pre-installation is not mandatory. For customer purchasing recommendations: SSD should preferably use TLC-grade flash (longer lifespan) in M.2 M-Key form factor. HDD uses 2x SATA interface, with single drive capacity up to 24TB. SSD brand references include Kingston, Samsung, and Lexar.

2. Basic Configuration

Q: How are the Ubuntu login username and password configured?

A: This device does not have an Ubuntu desktop environment; only CLI (command-line interface) is provided. This differs from the 8ch Mini which includes a desktop with NX Client. The system user account can log in directly to Ubuntu. A system user with a pre-configured password is provided. It is recommended to change the system user password via the Web interface as early as possible. The root user password is not provided externally; contact pre-sales or technical support if required.

Q: How do I activate the NX Server?

A: NX Server activation can be performed via the Web management interface using a browser, or through batch activation using Smart Tool. NX Server activation follows the same process as all NX services and can also be activated through a third-party client using the device's Web IP address.

Q: How do I distinguish between the two upgrade packages?

A: The Application Upgrade Package (e.g., OV_81.8.0.4-r3-NX) upgrades Milesight and NX Server/Client applications. The System Upgrade Package (e.g., OVSystem_81.8.0.4-r3) upgrades underlying components such as graphics card drivers, BIOS, and MCU firmware. During system detection, upgrades are applied sequentially. It is generally recommended to upgrade both to the latest version.

Q: What is the biggest difference between this product and the old SE0201?

A: Three main points: (1) More power-efficient (9W vs 35W); (2) More rugged (-10 to 55C vs 0 to 35C); (3) Easier maintenance (full Web-based management vs minimal Web capabilities on the old model). Additionally, CPU, memory, network ports, storage, and capacity are all upgraded, and the 32ch model adds RAID1 data protection.

Q: How do I choose between 16ch and 32ch?

A: 16ch: For small-to-medium projects focused on recording and management, no RAID requirement, budget-sensitive. 32ch: For medium-to-large projects requiring 32-channel access and RAID1 data protection.

Q: Does it support local display / local Client?

A: No. The 16ch/32ch models are pure Server form factors with no Ubuntu desktop and no local NX Client. The dual HDMI ports are for testing and debugging only.

Q: Does it support dual network ports? What can customers use them for?

A: Yes, dual 2.5G network ports are supported. They can be used for business/maintenance network isolation, dual-link backup, or link aggregation for bandwidth expansion.

Q: Can it be marketed as an "AI Server"?

A: Not recommended. A more accurate description is "an edge server that ingests AI camera metadata and manages events and search capabilities on the NX platform."

Q: What is Smart Tool Lite? How is it different from Smart Tool?

A: Smart Tool Lite is a Web-based built-in tool for batch camera operations including camera search, batch IP modification, and batch initialization. Smart Tool is a desktop application for device discovery, activation, and IP configuration.

Q: Is there a PoE version?

A: Not currently. A PoE-equipped model was planned early on but is not available for sale at this time.

3. Specifications

Q: What is the actual power consumption?

A: Typical power consumption is 9W (without drives) and maximum is 39W (with 2x HDD). This is a key selling point compared to the older model (35W/60W) and competitors.

Q: Where is the NX analytics database stored?

A: By default, the analytics database resides on the HDD. After installing an M.2 SSD, it can be migrated to the SSD for faster retrieval and playback. The default database path on HDD1 is: /mnt/sata_1/data/[MAC]/data. When using SSD1, the path is: /mnt/ssd_1/data/[MAC]/data.

4. Troubleshooting

Q: Network is abnormal and I cannot log in to the Web interface?

A: First confirm that the network cable, IP address, and power supply are normal. Connect a monitor to access the CLI and verify the network configuration. Use Smart Tool to search for the device and verify network information. Check whether link aggregation is enabled, which may cause the IP address to change.

Q: A brand-new SSD/HDD is not recognized or cannot be formatted?

A: Power off the device, reseal the drive securely and tighten the screws, then upgrade to the latest firmware version. Check the Storage page to confirm whether the drive can

be formatted. If the issue persists, investigate from the backend. Important: Do NOT format storage using command-line or low-level tools. Always use the Web interface for storage management.

Q: The IP found by Smart Tool does not match expectations?

A: Since this device has dual network ports, in Independent Mode, Smart Tool may discover two IP records (one for each port). If the discovered IP differs from both port IPs, this was a known bug that has been fixed. Upgrade the firmware to the latest version first.

Q: The Server is inaccessible or the Web interface crashes?

A: Upgrade to the latest firmware first, as this resolves most issues. If the problem persists, you can reformat the SSD through the Web interface. Important: Do NOT format the SSD using command-line tools. Always use the Web interface.

Q: How do I perform a hardware reset? What happens to passwords and activation?

A: Two reset methods are available: (1) Factory Reset: Hold the Reset button before powering on, continue holding until the status LED flashes 10 times and turns solid. This restores factory defaults and clears all data. (2) Configuration Reset: Press and hold Reset for 10 seconds while the device is running. This restores configuration settings while retaining the IP address and user information.

5. Storage & Network

Q: How do I add additional storage to the device?

A: Local storage includes 2x HDD (single drive up to 24TB) + 2x M.2 SSD. Additional capacity can be expanded via Web-mounted NFS/SMB NAS.

Q: Network was misconfigured and the device is unreachable. How do I recover?

A: Use the Reset button to perform either "Configuration Reset" (retains IP and user information) or "Factory Reset" (clears all data). Understand the difference between these two actions before proceeding.

6. RAID1 (32ch Model Only)

Q: What RAID support is available? Does the 16ch model support RAID?

A: Only the 32ch model (SE0232R) supports RAID1 (2x HDD). The 16ch model does not support RAID. RAID1 covers the complete lifecycle including pool creation, online operation, scrubbing, degraded mode, candidate disk repair, and resilvering - all managed through the Web interface. RAID5 is not available in this release; do not promise RAID5 to customers.

Q: If one drive fails, will data be lost?

A: No. RAID1 uses mirroring; both drives back up each other. If one drive fails, data remains on the other drive. The system enters DEGRADED status and prompts for drive replacement. After inserting a compatible drive, execute Repair to rebuild redundancy and restore ONLINE status.

Q: Can RAID drives removed from another device be used in this unit?

A: Yes, but the process depends on the situation and must follow Recover first, then Repair: (1) A single foreign RAID1 member (from the same Milesight model): The system detects the foreign signature and will not automatically merge it. Use Recover RAID Group to import it as a DEGRADED pool, then insert a compatible drive to Repair and

restore redundancy. (2) Both members of the same foreign RAID1 group present: Can be recovered to an ONLINE pool after confirmation, with both members immediately locked under local protection. (3) Multiple different foreign RAID1 groups: The system will prompt a conflict and require selecting one group to retain data; it will NOT merge different foreign groups. (4) Third-party ZFS or non-local signature drives: Only controlled formatting is available; data recovery is not supported.

Q: What if recovering a foreign drive fails or pre-check does not pass?

A: Before recovery, the system performs a pre-check. If it fails, the reason is displayed and the operation returns to the foreign group selection or conflict list. The system will NOT silently format or automatically create a new pool. After single-member recovery, the pool is only DEGRADED; it will not automatically rebuild. Redundancy must be restored through subsequent Repair.

Q: Can RAID1 drives be read on another Linux computer?

A: Yes. RAID1 uses ZFS mirroring. The drive can be mounted on a Linux computer with ZFS installed (version 2.2.2 or higher) and remains readable. This is convenient for offline forensic analysis or data recovery on a different machine.

Chapter 9. Services

Milesight provides customers with timely and comprehensive technical support services. End-users can contact your local dealer to obtain technical support. Distributors and resellers can contact directly with Milesight for technical support.

Technical Support Mailbox: support@milesight.com

Web: <https://www.milesight.com/security/>

Online Problem Submission System: <http://www.milesight.com/service/feedback.asp>

MILESIGHT CHINA

TEL: +86-592-5922772

Add: Building C09, Software Park Phase III, Xiamen 361024, Fujian, China