Milesight OpenVision Server Mini User Manual

Version: V1.0

Date: 2026-02-27

Chapter 1. Introduction....4
1.1 Copyright Statement....4
1.2 Safety Instruction....4
1.3 EU Conformity Statement....5
1.4 Revision History....5
Chapter 2. Product Description....6
2.1 Product Overview....6
2.2 System Requirements....6
2.3 Hardware Overview....6
2.4 Related Documents....7
Chapter 3. Configuration Flow....9
Chapter 4. Device Access....11
4.1 Inserting SSD(s) and Powering On....11
4.2 Assigning an IP Address....11
4.1 Assigning an IP Address Using Smart Tools....11
4.2 Assigning an IP Address via Browser....14
Chapter 5. Web Settings....17
5.1 Overview....17
5.1.1 Key Features....17
5.1.2 Login....17
5.2 Media....18
5.2.1 Audio....18
5.3 Network....20
5.3.1 Basic....20
5.3.2 Advanced....26
5.4 Storage....26
5.4.1 Storage Management....26
5.5 Event....29
5.5.1 Basic Event....29
5.6 VMS Edge....33
5.7 System....40
5.7.1 System Setting....40

5.7.2 Security..... 43
5.7.3 Logs..... 50
5.7.4 Maintenance.....51
Chapter 6. Integration with NX Server..... 55
6.1 Add Device.....55
6.2 Alarm I/O.....56
6.3 Audio Input.....59
6.4 Play Sound.....61
6.5 Reboot.....62
6.6 Web Page..... 63
6.7 Firmware Upgrade..... 64
6.8 Device Info.....65
Chapter 7. FAQ..... 67
7.1 General Configuration.....67
7.1.1 Ubuntu Login..... 67
7.1.2 Device Activation..... 67
7.2 Common Issues.....67
7.2.1 IP Conflicts.....68
7.2.2 Server Inaccessibility..... 68
7.2.3 Webpage Crash.....68
7.2.4 Device Reset..... 68
7.2.5 Password Reset.....70
Chapter 8. Services..... 74

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).

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 Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss. The precaution measures are divided into “Warnings” and “Cautions”

Warnings: Serious injury or death may be caused if any of these warnings is neglected.

- This installation must be conducted by a qualified service person and should strictly comply with the electrical safety regulations of the local region.
- To avoid risk of fire and electric shock, do keep the product away from rain and moisture before installed.
- Do not touch components such as heat sinks, power regulators, and processors, which may be hot.
- Source with DC 12V or PoE+ (802.3at) .
- Please make sure the plug is firmly inserted into the power socket.
- If the product does not work properly, please contact your dealer. Never attempt to disassemble the product by yourself.

Cautions: Injury or equipment damage may be caused if any of these cautions are neglected.

- Make sure that the power supply voltage is correct before using the product.
- Do not store or install the device in extremely hot or cold temperatures, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- Only use components and parts recommended by manufacturer.
- Do not drop the device or subject it to physical shock.
- To prevent heat accumulation, do not block air circulation around the device.

- Use a soft, dry cloth to clean the surface of the device. Stubborn stains can be removed using a soft cloth dampened with a small quantity of detergent solution, then wipe dry.
- Do not use volatile solvents such as alcohol, benzene or thinners as they may damage the surface finishes.
- Save the package to ensure availability of shipping containers for future transportation.

1.3 EU Conformity Statement

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info.

1.4 Revision History

Table 1. Revision History

Version	Software Version	System Version	Revision Content	Release Date
V1.0	OV 81.8.0.4-r2-NX	OVSystem 81.8.0.4-r1	First Release	February 2026

Chapter 2. Product Description

2.1 Product Overview

What is Milesight OpenVision Server Mini?

Milesight Openvision Server Mini is an all-in-one intelligent monitoring workstation, offering a pre-configured, plug-and-play surveillance platform with the **Network Optix VMS 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 Mini is ideal for outdoor edge deployment scenarios, providing a streamlined, cost-effective, and smart security solution.

2.2 System Requirements

Operating System: Windows XP/Windows 7/8/10/11/Server 2000/Windows Server 2008

CPU: 1.66GHz or higher

RAM: 1G or higher

Graphic Memory: 128MB or more

Internet Protocol: TCP/IP (IPv4/IPv6)

Web Browsers: Support Micro Edge/ Google Chrome/ Safari/ Mozilla Firefox Browser

2.3 Hardware Overview

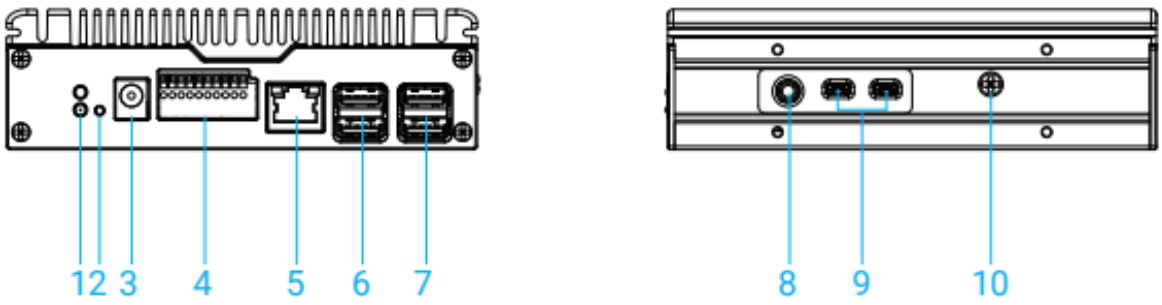
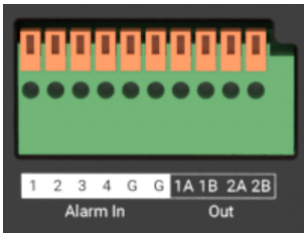


Table 2. Interfaces Description

No.	Interfaces	Key Specifications	Function & Usage
1	Indicator Light	2 (Power & Alarm Light)	Shows the device's power and alarm status.
2	Reset Button	1	Restores the device to factory default settings.
3	Power Supply	DC 12V±15% (5525 DC power plug)	Connects the external power adapter to supply power.
4	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).
5	Ethernet Port	1*2500Mbps RJ45 Ethernet Port, support POE PD	Supports network connectivity and PoE+ power receiving via Ethernet cable.
6	USB Interface	3*USB 3.0	Used to connect various external devices such as a mouse and keyboard, enabling data transmission and device control.
7		1*USB 2.0	
8	Audio	1* 3.5mm Headphone Jack with Microphone Input (4-pole, TRRS, CTIA Standard)	Supports two-way audio via headset with microphone.
9	Micro HDMI Port	2	Connects to monitors for high-resolution video output. Supports dual-display mode.
10	Grounding Hole	1	Connects a grounding wire to prevent static damage.

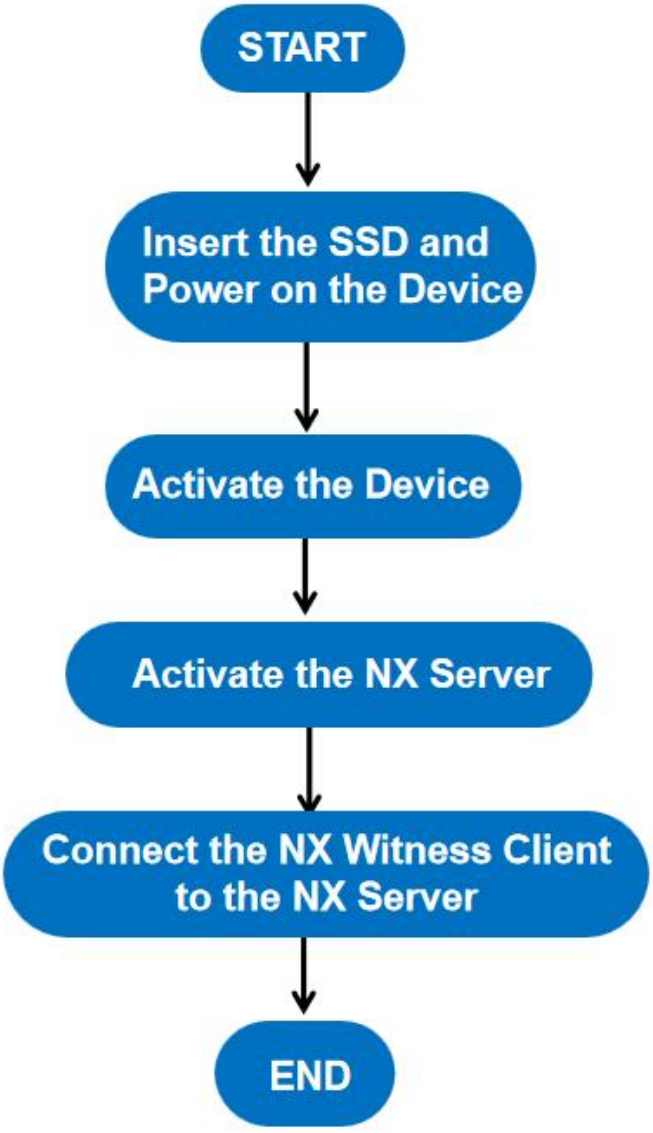
2.4 Related Documents

Table 3.

Document Type	Link
Datasheet	https://resource.milesight.com/milesight/security/document/datasheet/ipc/open-vision/milesight-openvision-server-mini-datasheet-en.pdf
Quick Start Guide	https://resource.milesight.com/milesight/security/document/user-manual/openvision/milesight-openvision-server-mini-quick-start-guide-en.pdf
How to Guide	https://resource.milesight.com/milesight/security/document/user-manual/openvision/how-to-set-up-milesight-openvision-server-mini.pdf

Chapter 3. Configuration Flow

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



More configuration details are shown in the following table.

Table 4. Description of flow

Configuration	Reference
Insert SSD and Power on the Device	4.1 Inserting SSD(s) and Powering On *(page 11)*
Activate the Device	4.2 Assigning an IP Address *(page 11)*

Configuration	Reference
Activate the Nx Witness Server	5.6 VMS Edge *(page 33)*
Connect to the Nx Witness Client	5.6 VMS Edge *(page 33)*

Chapter 4. Device Access

4.1 Inserting SSD(s) and Powering On

To ensure the device functions properly, please make sure the SSD is installed before activating the device.

Step 1: Open the rear panel and then insert up to two SSDs into the slots.

Step 2: Attach the heat conduction pad to each SSD.

Step 3: Power on the device.

Note:

- If you need more detailed guidance, please refer to the Quick Start Guide or consult our support team.

4.2 Assigning an IP Address

The product must be assigned an IP address to be accessible. The default IP address of Milesight OpenVision Server Mini is 192.168.5.190. You can either change the IP address of the device via Smart Tools or browser. Please connect the device in the same LAN of your computer.

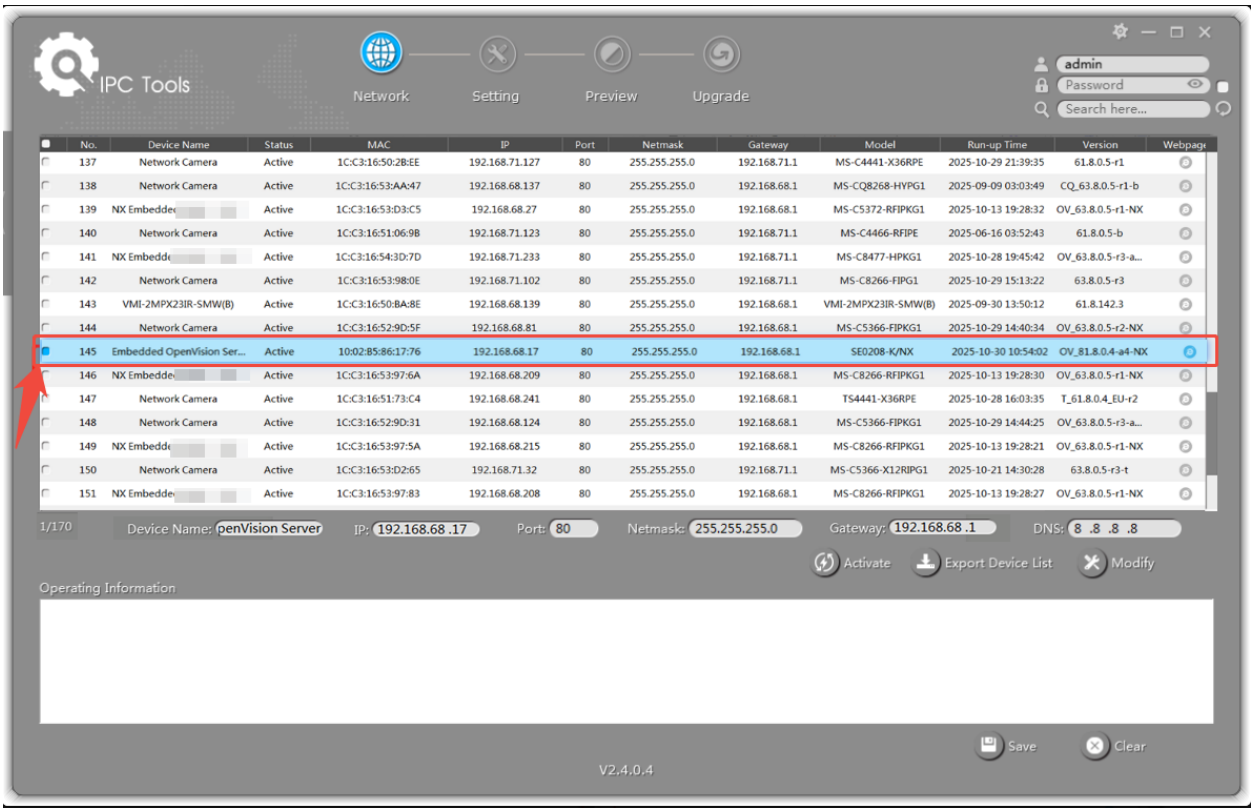
4.1 Assigning an IP Address Using Smart Tools

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;

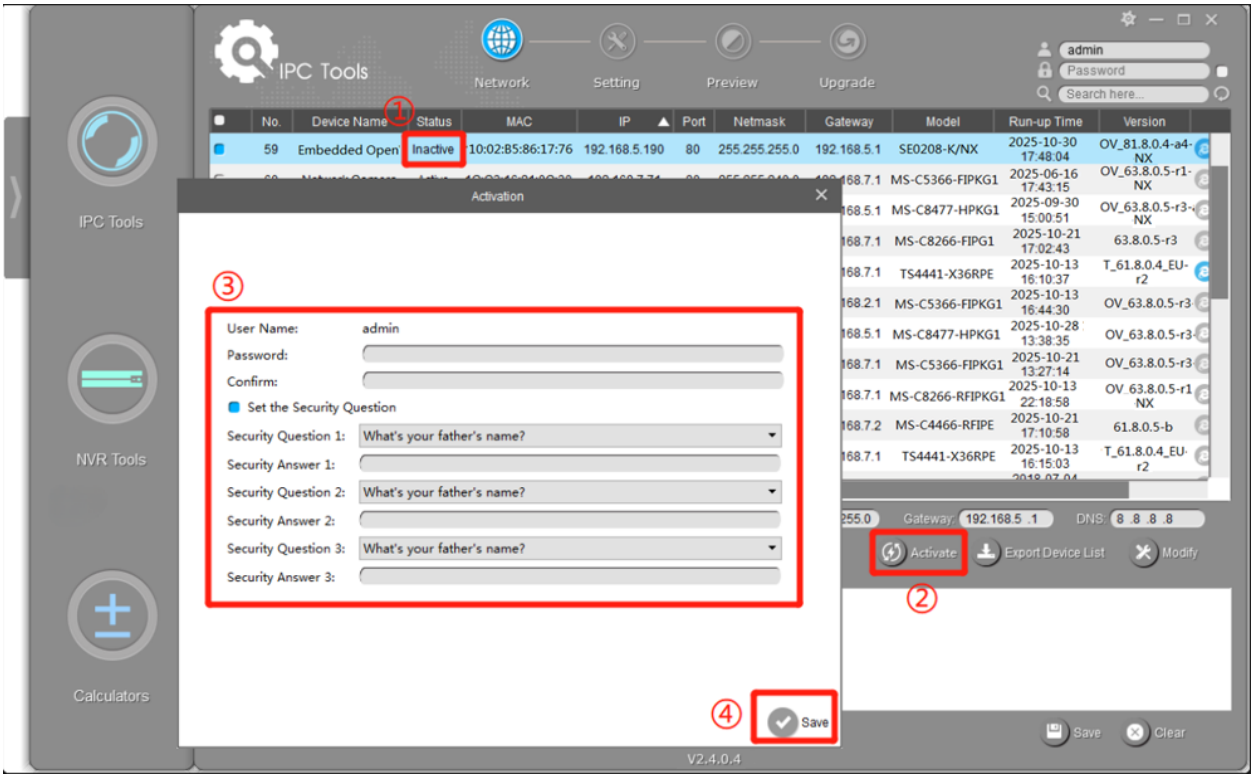
Step 3: Select the device according to the MAC addresses;



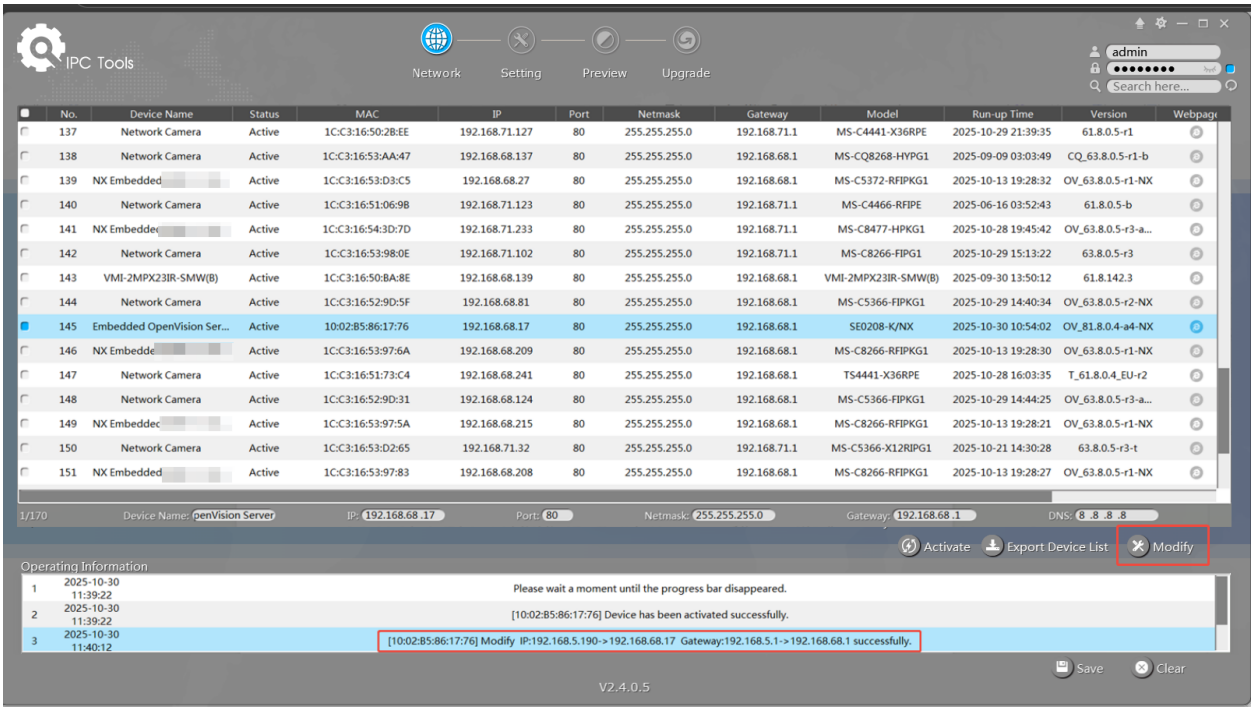
Step 4: If the selected device shows "Inactive" in the status bar, click "Activate" to set the password when using it for the first time. You can also set the security questions when activating the device in case that you forget the password (You can reset the password by answering three security questions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

Note:

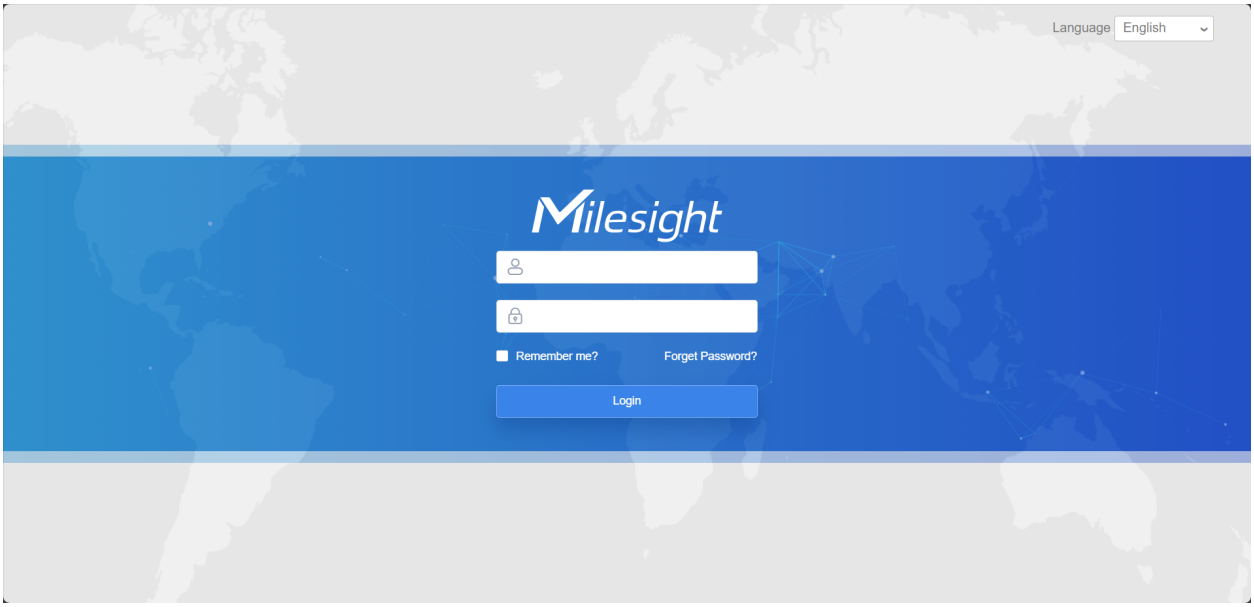
Password must be 8 to 32 characters long, contain at least one number and one letter.



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. The Internet Explorer window will pop up.



More usage of Smart Tools, please refer to the ***Smart Tools User Manual***.

4.2 Assigning an IP Address via Browser

If the network segment of the computer and that of the device are different, please follow the steps to change the IP address:

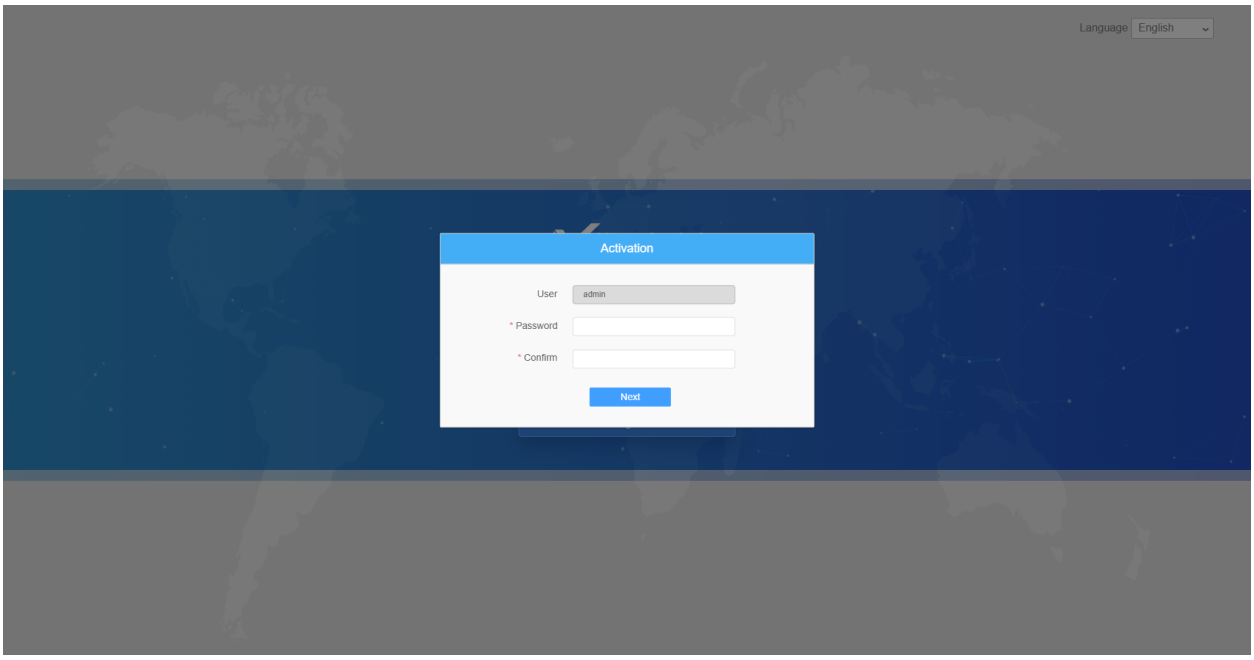
Step 1: Change the IP address of computer to 192.168.5.0 segment, here are two ways as below:

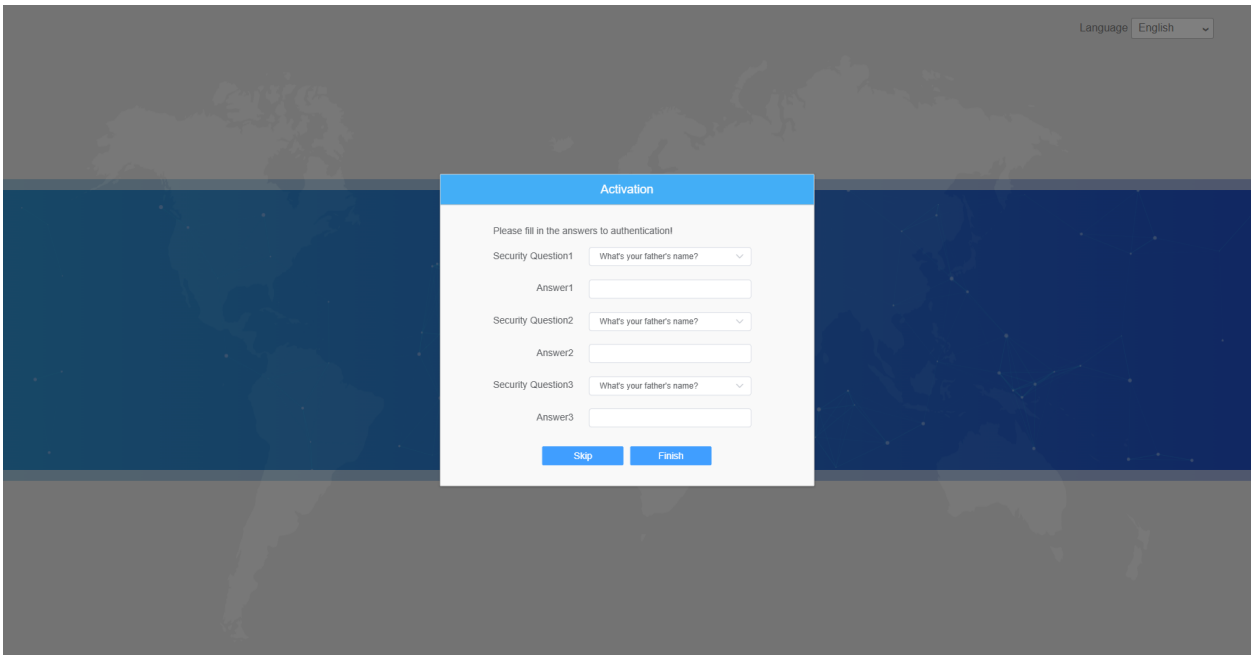
a. Start-->Control Panel-->Network and Internet Connection-->Network Connection-->Local Area Connection, and double click it;

b. Click “Advanced”, and then click “IP settings”--> “IP address”--> “Add”. In the pop-up window, enter an IP address that in the same segment with Milesight OpenVision Server Mini (e.g. 192.168.5.61, but please note that this IP address shall not conflict with the IP address on the existing network);

Step 2: Start the browser. In the address bar, enter the default IP address of the Milesight OpenVision Server Mini: http://192.168.5.190;

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



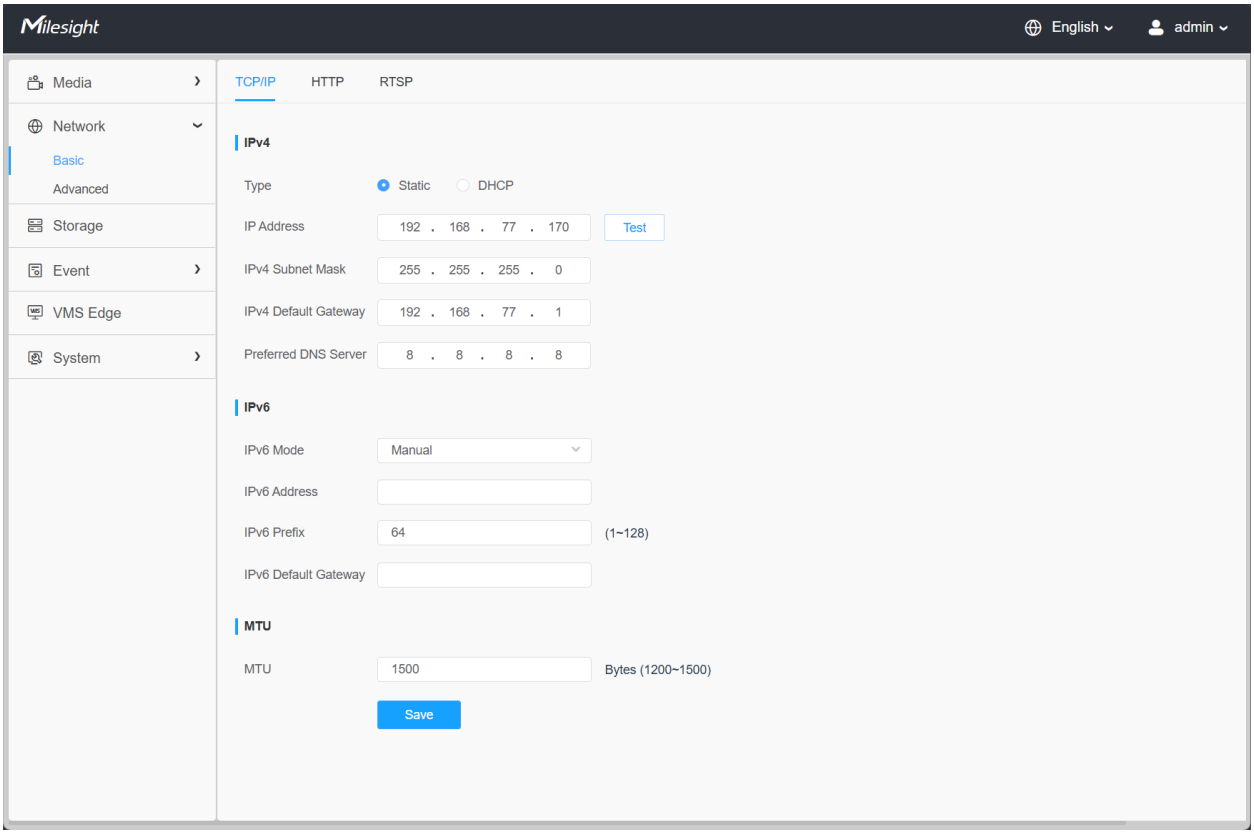


Note:

- 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 5. Web Settings

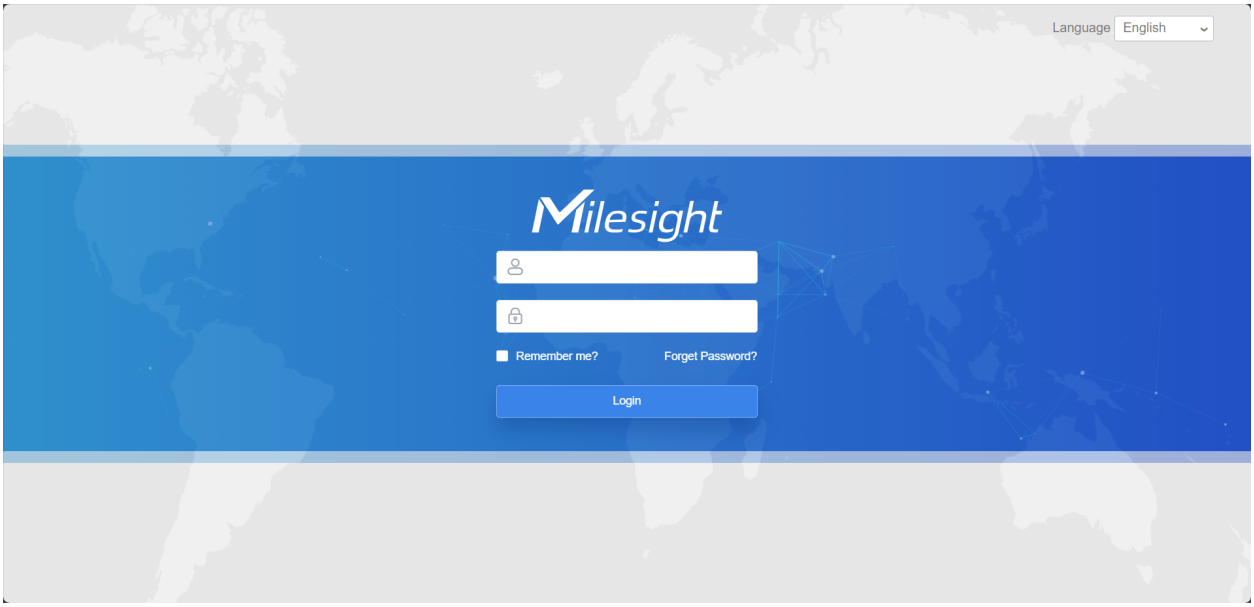
5.1 Overview

5.1.1 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 firmware upgrades.
- Supports basic maintenance functions, such as scheduled reboot and factory reset.
- Supports ONVIF server (can be added to Nx 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.
- Supports automatic time synchronization, IP whitelist, and system logs.
- Supports multiple languages.
- Supports Nx Witness Server management tools and configuration optimization.
- Supports Nx Witness Client management tools.

5.1.2 Login



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

1. The device has been equipped with the SSD.

2. The device has been activated and assigned a valid IP address.

For detailed activation steps, please refer to Chapter 4 *(page 11)*.

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.

5.2 Media

5.2.1 Audio

5.2.1.1 Audio

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

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

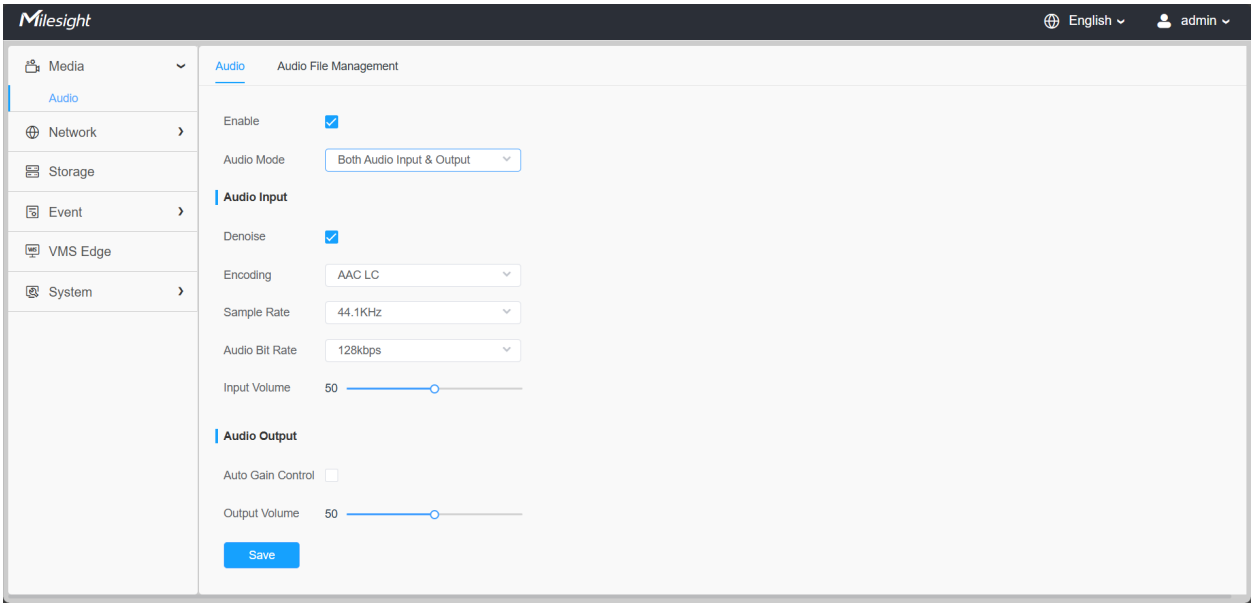
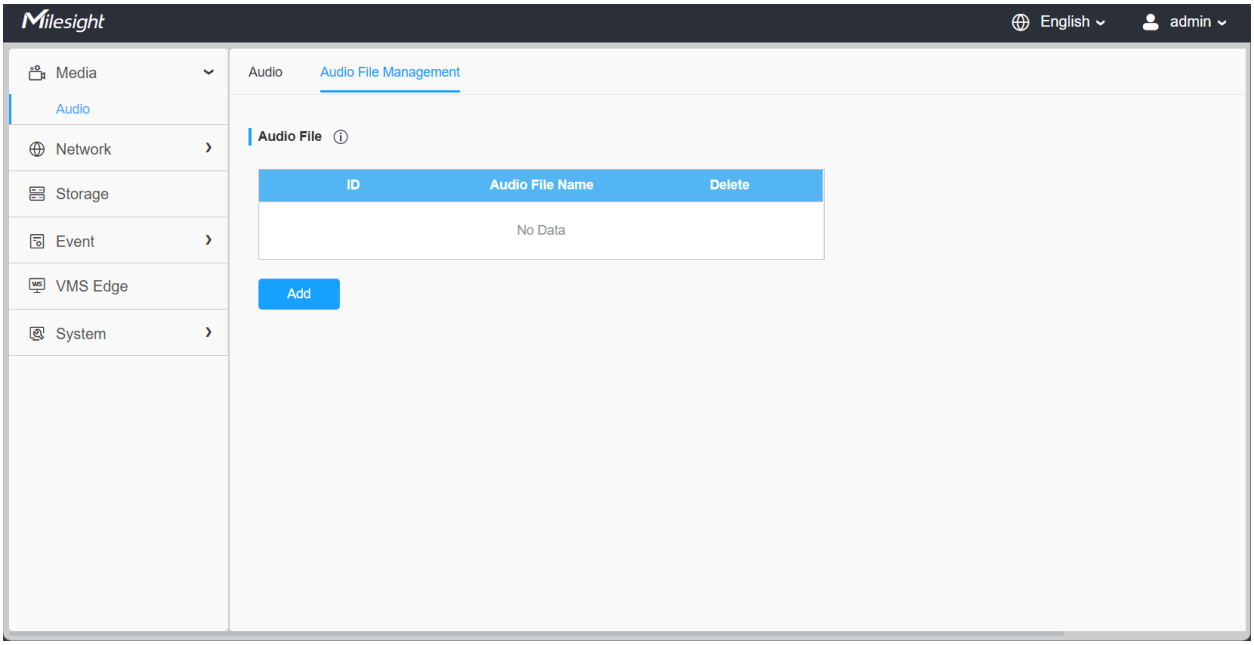


Table 5. Description of the buttons

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.

5.2.1.2 Audio File Management

You can upload up to 5 audio files manually to 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!

5.3 Network

5.3.1 Basic

5.3.1.1 TCP/IP

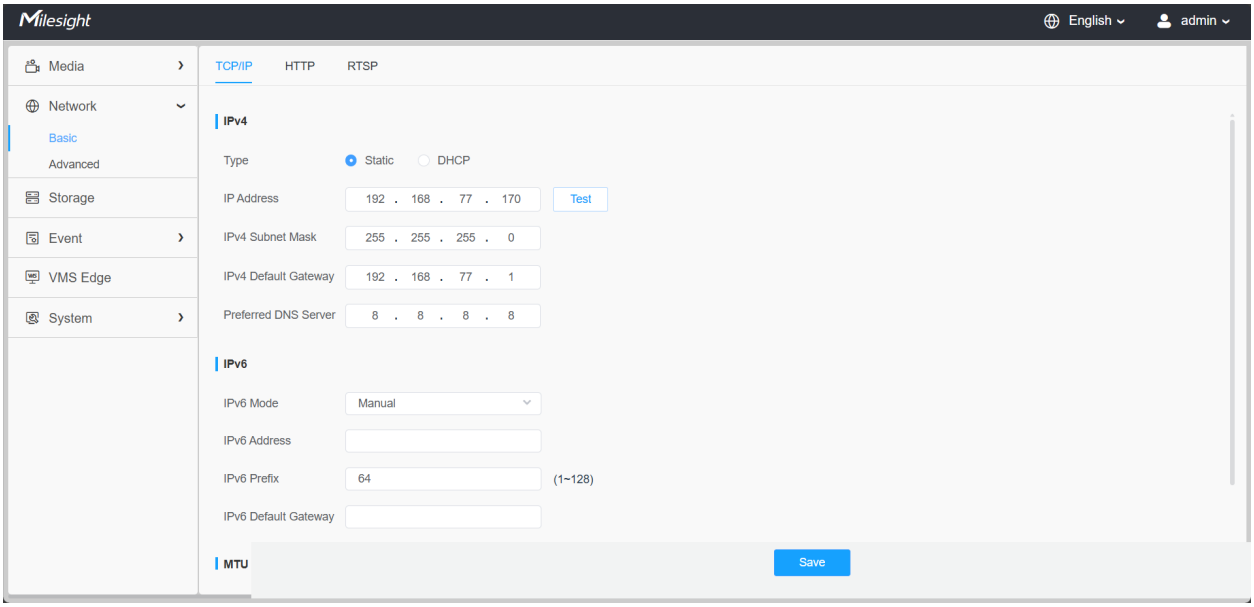


Table 6. Description of the buttons

Parameters	Function Introduction
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/Route Advertisement/ 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	Save the configuration.

5.3.1.2 HTTP

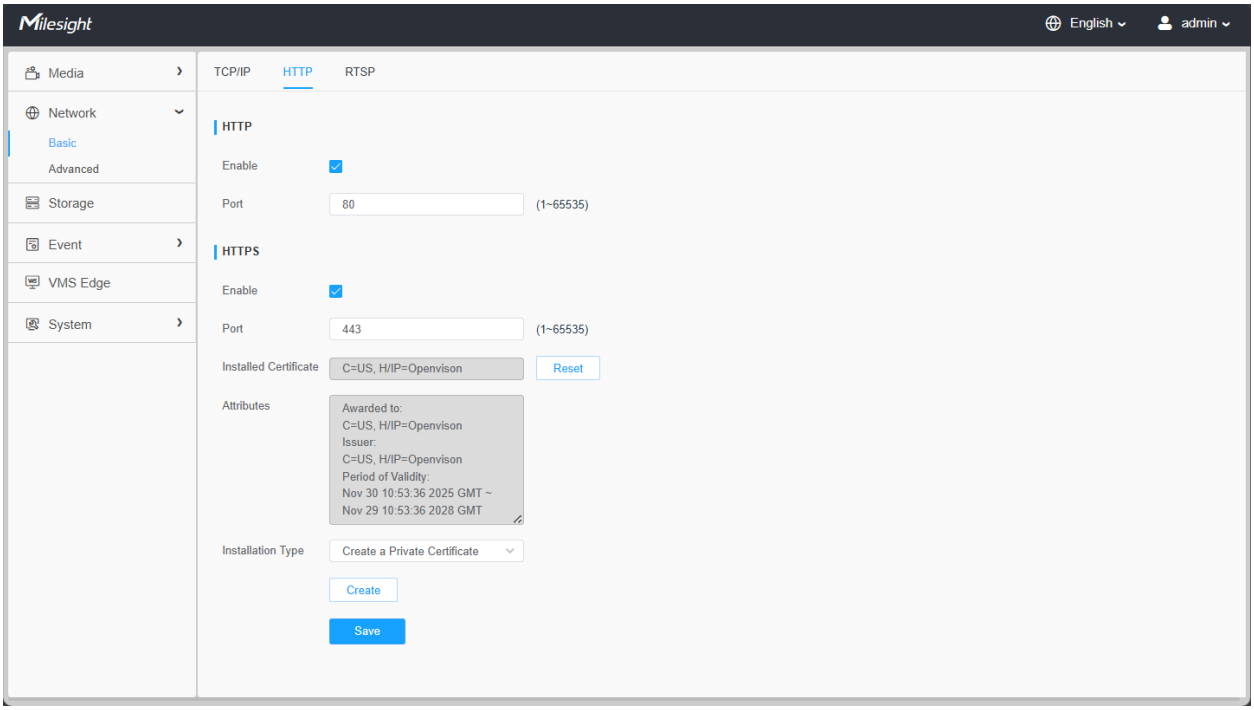


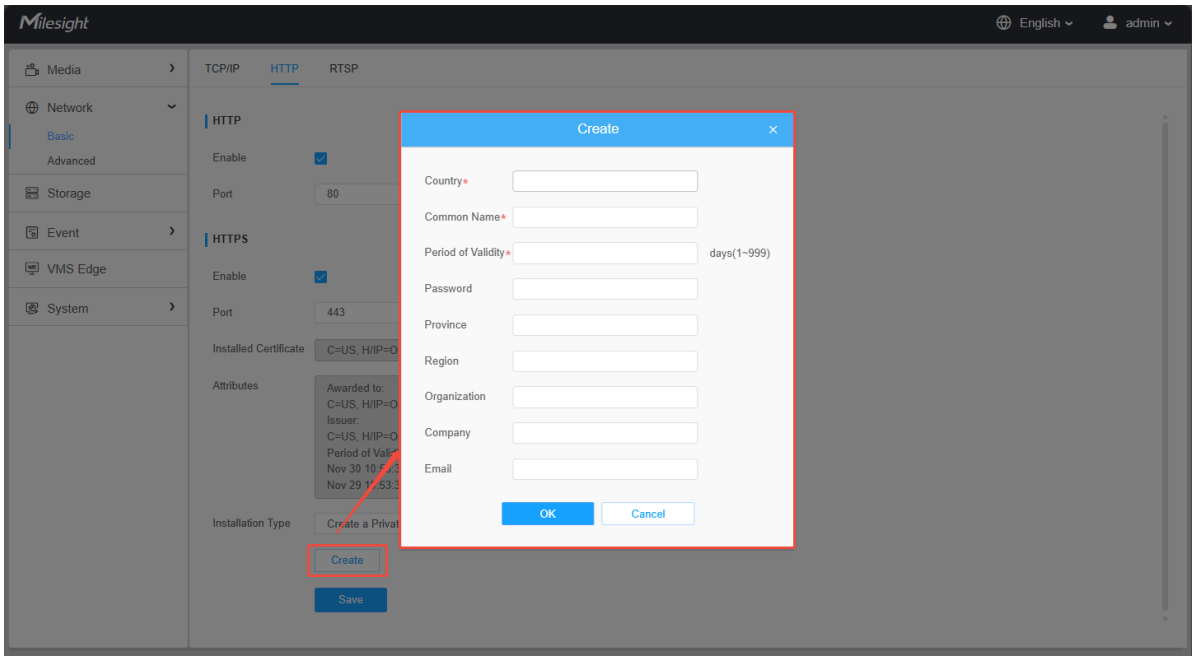
Table 7. Description of the buttons

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:

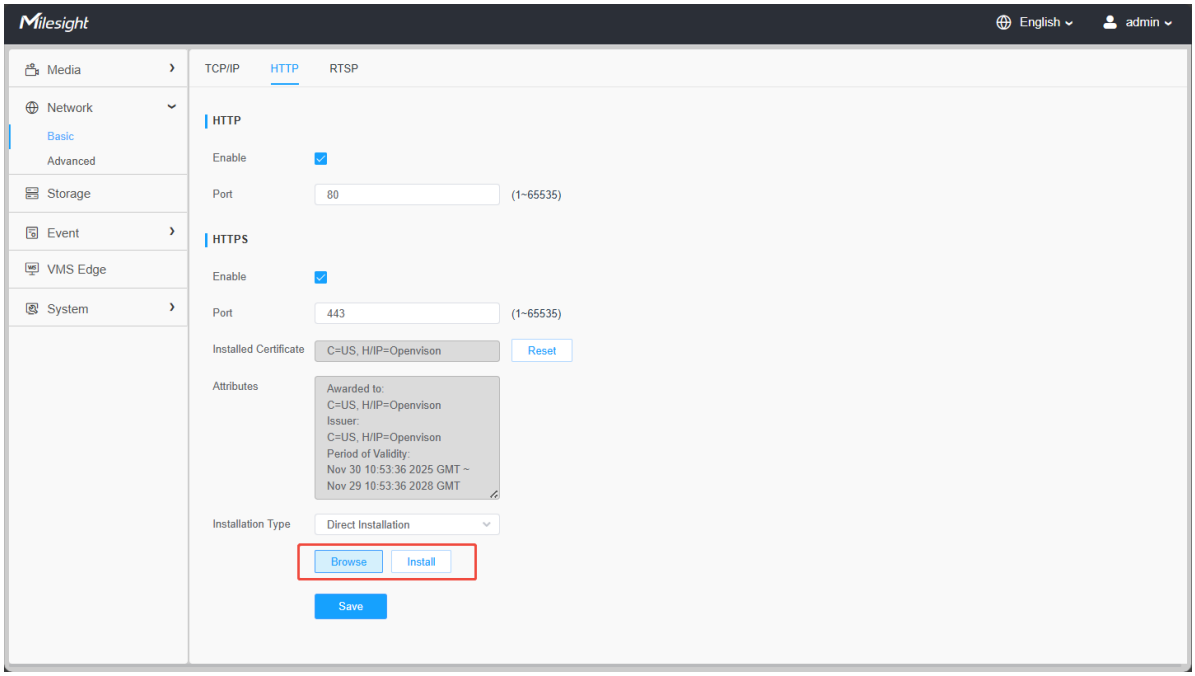
- **Create a Private Certificate:**

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.

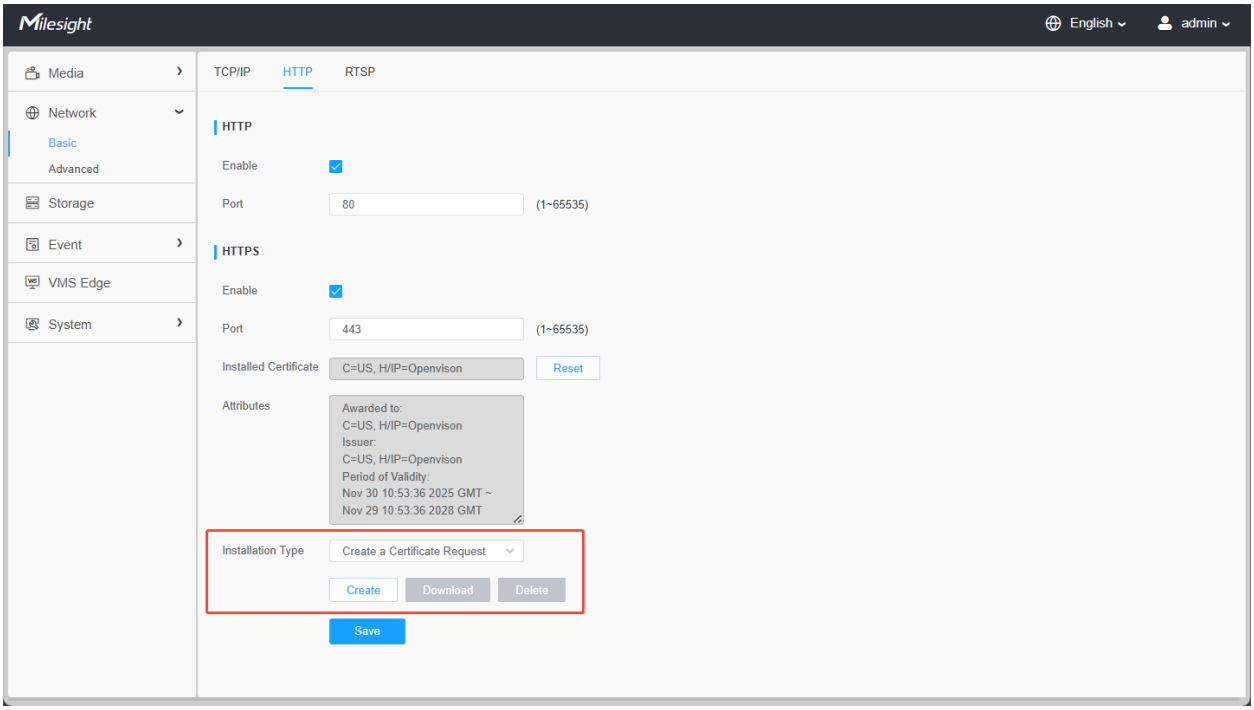


- **Create a Certificate Request**:

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 Mini by inputting https://ip:port via the web browser.

5.3.1.3 RTSP

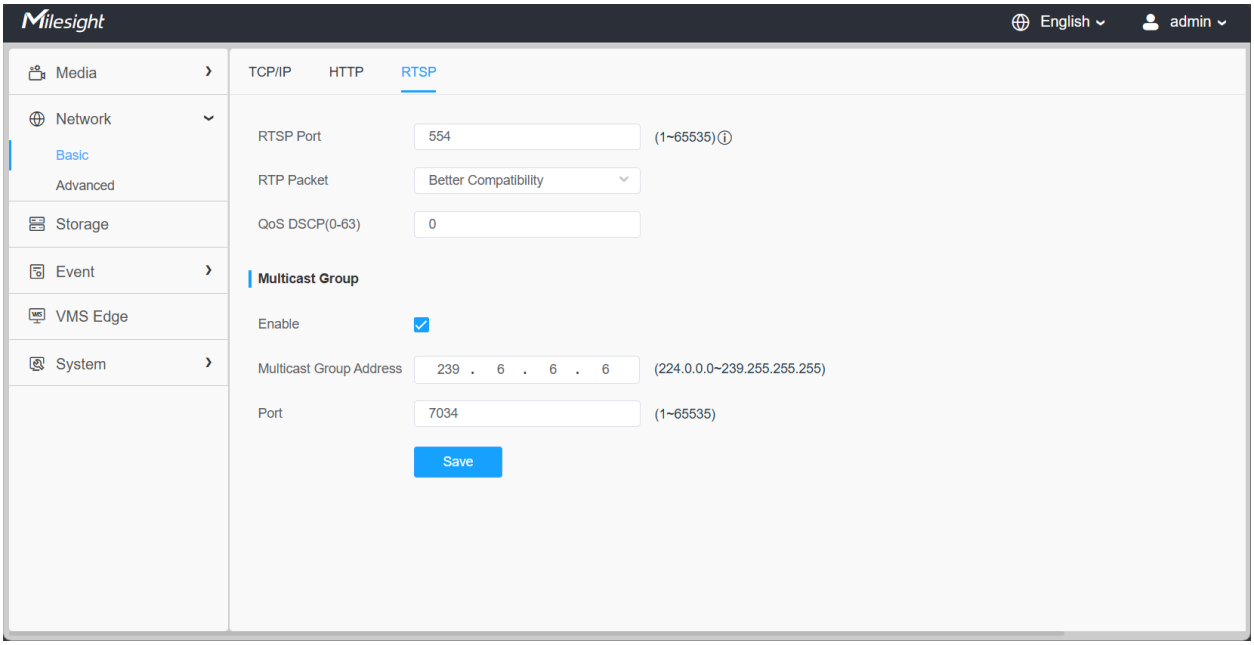


Table 8. Description of the buttons

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	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.

5.3.2 Advanced

5.3.2.1 ONVIF

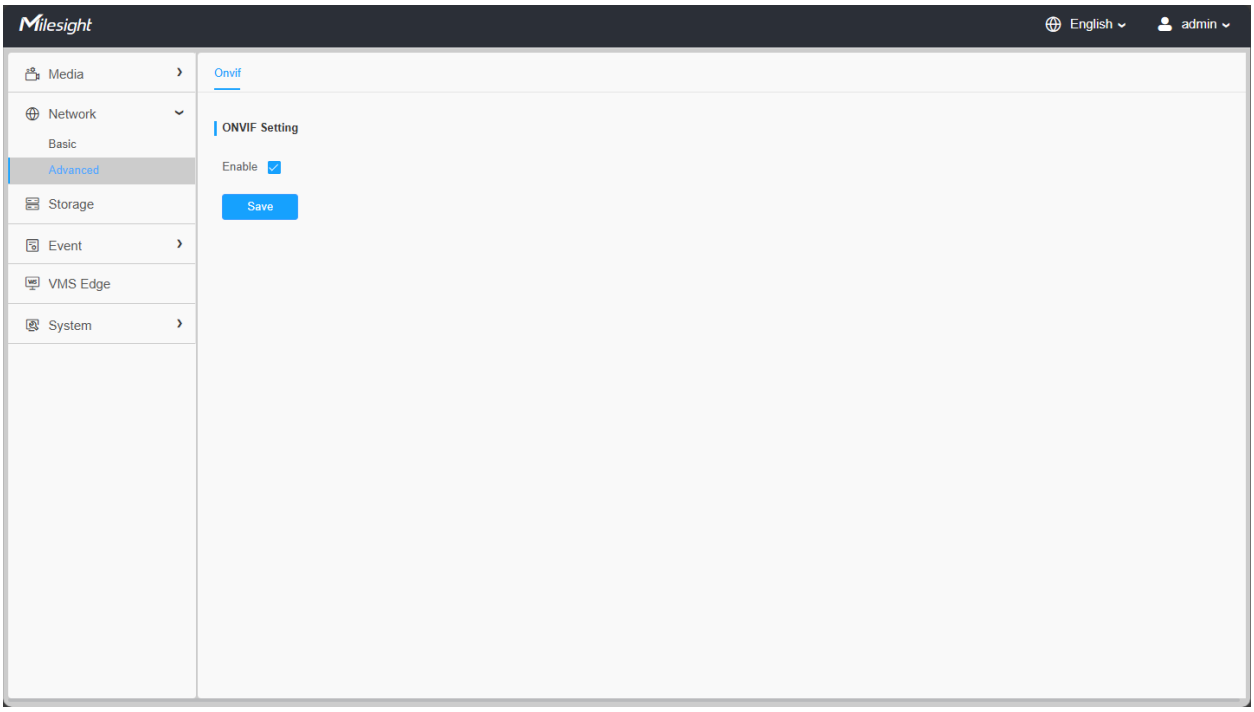


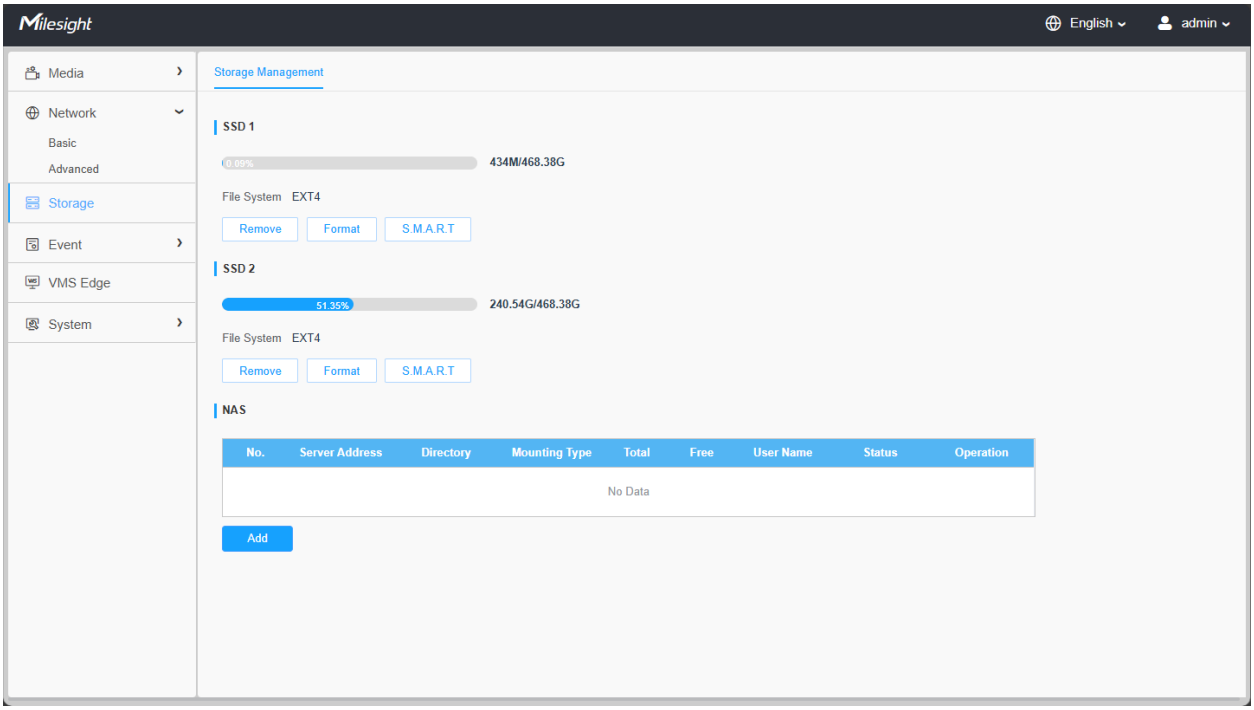
Table 9. Description of the buttons

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.

5.4 Storage

5.4.1 Storage Management

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



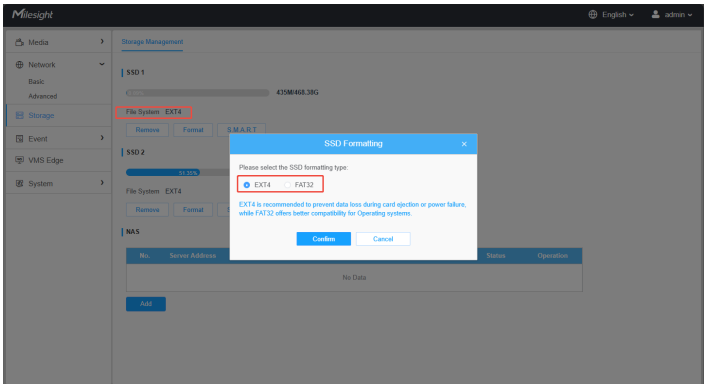
After that, it will be automatically detected , and the detailed information of the SSD will be displayed on the SSD bar.

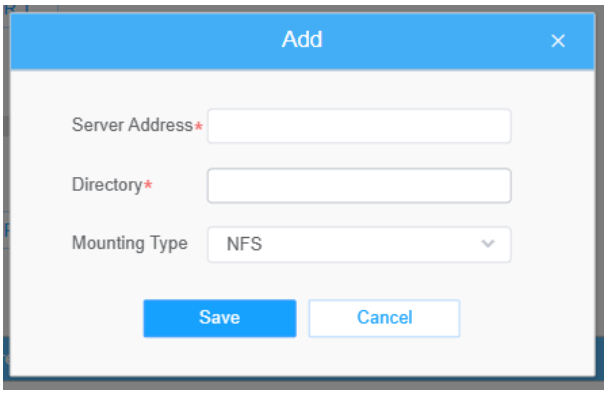
Step 2: In the SSD bar, you can click on Remove to remove the SSD or click on Format to format the SSD and clear all files on it. You can also click on S.M.A.R.T to check the health information of SSD.

[Warnings]:

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

Table 10. Description of the buttons

Parameters	Function Introduction
SSD	**Format:** Format SSD, the files in SSD will be removed. It supports two file system formats including EXT4 and FAT32, and EXT4 is recommended to prevent data loss during card ejection or power failure, while FAT32 offers better compatibility for Operating systems.  **Remove:** Remove SSD. **S.M.A.R.T:**You can click S.M.A.R.T to check SSD health information.

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.  **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.

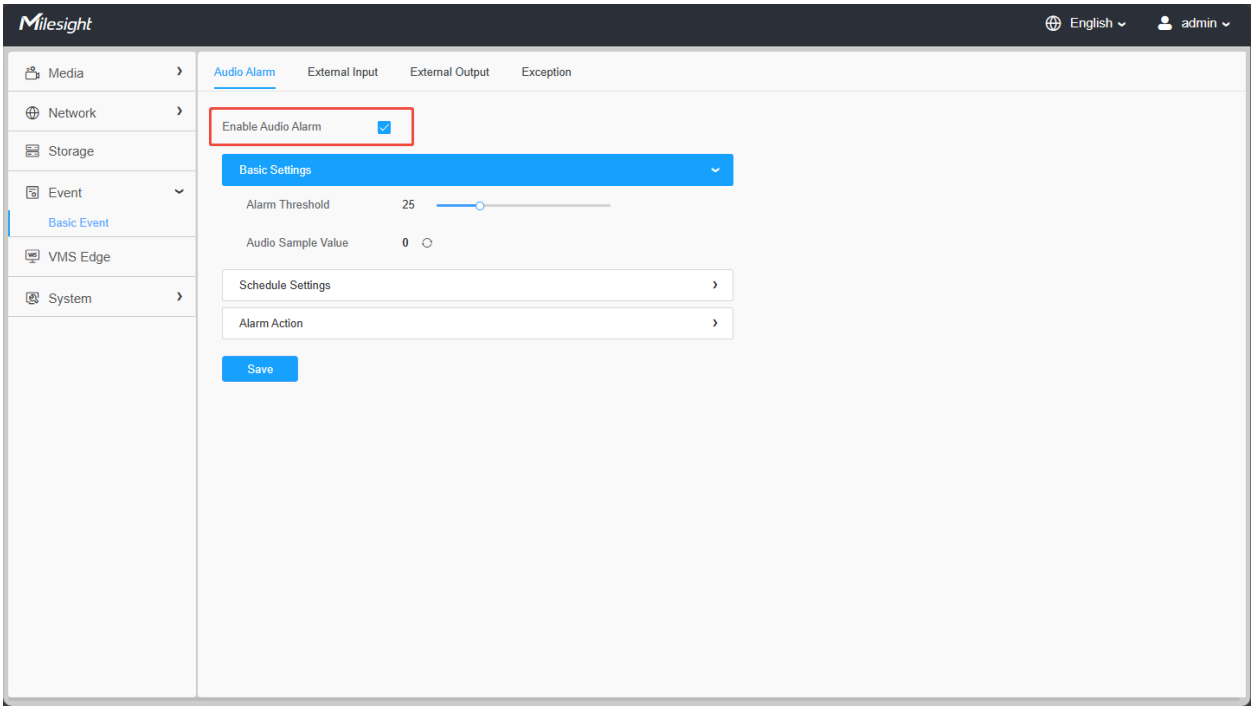
5.5 Event

The event provides advanced, accurate smart video analytics for Milesight network cameras. It enhances the performance of network cameras through basic events and VCA events, enabling a comprehensive surveillance system and quicker response of cameras to different monitoring scenes.

5.5.1 Basic Event

5.5.1.1 Audio Alarm

Check the check box to enable the Audio Alarm function.



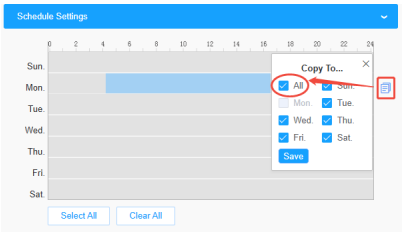
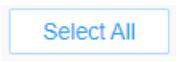
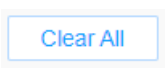
[Basic Settings]

Table 11. 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 12. Description of the buttons

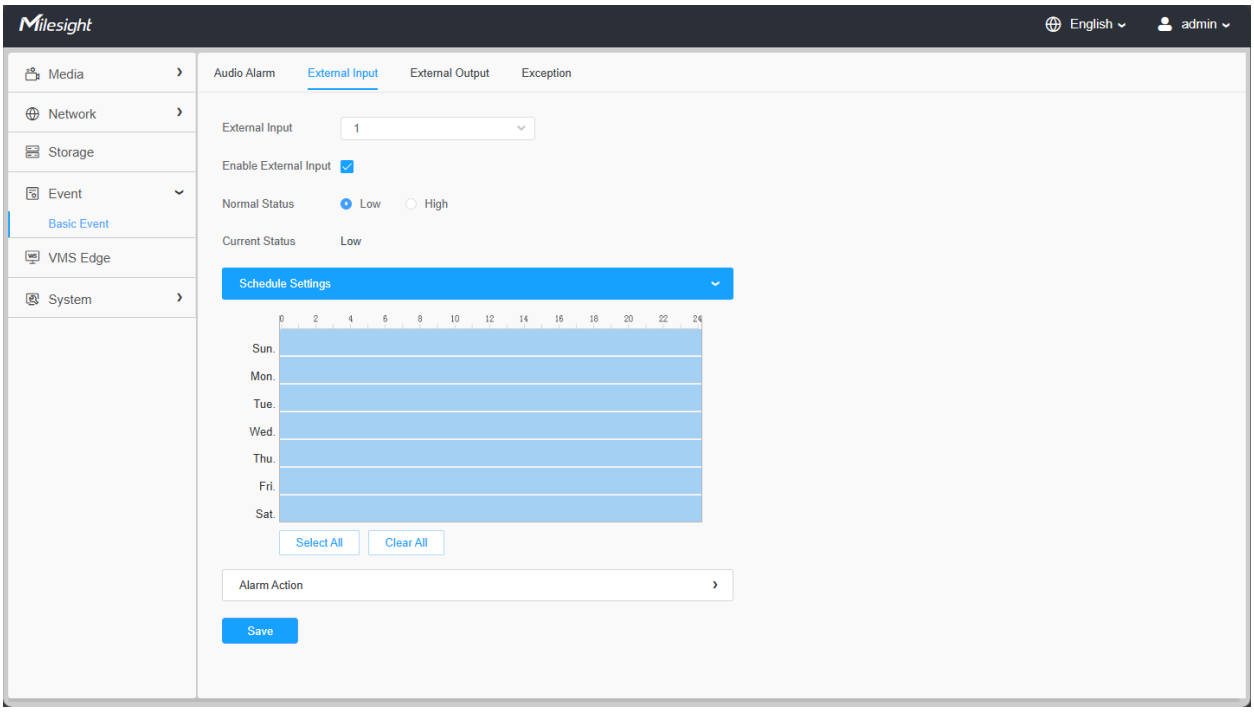
Parameters	Function Introduction
	Copy the schedule area to another date. The "All" button is handy to copy today's schedule to all days.
	Select all schedule.
	Clear all schedule.

[Alarm Action]

Table 13. 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

5.5.1.2 External Input



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

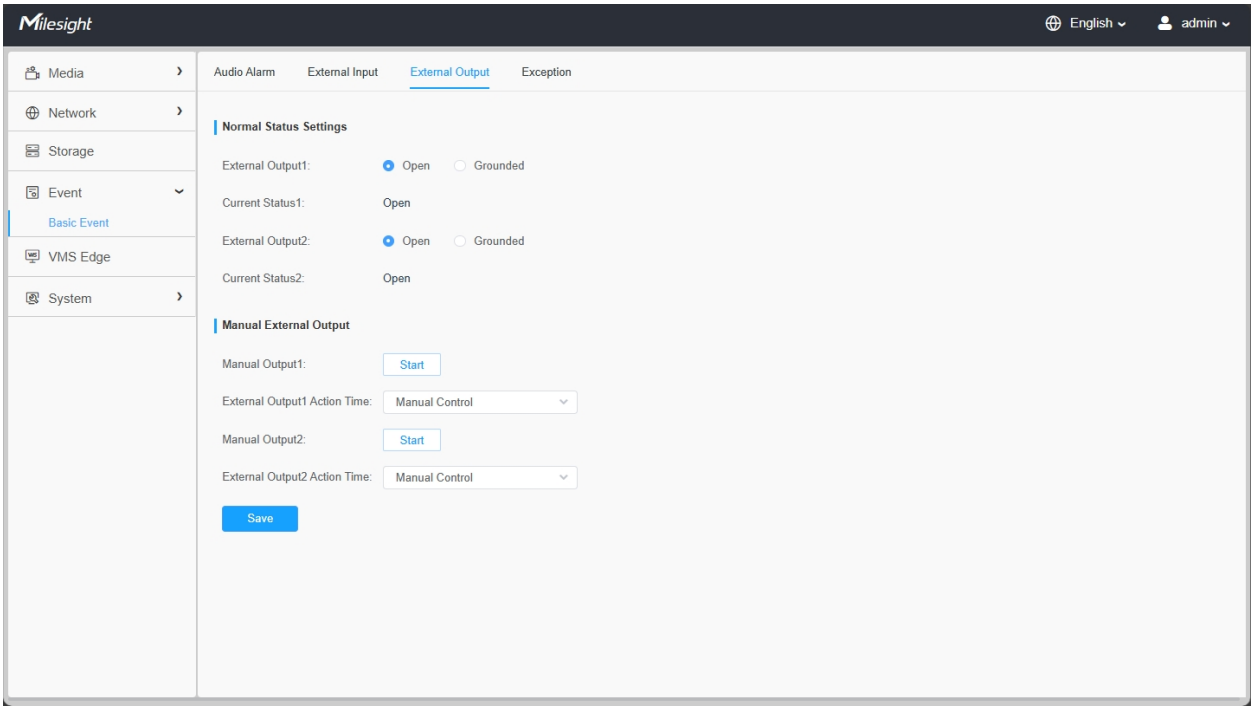
Step 2: Please set the **Normal Status** firstly, when the **Current Status** is different with **Normal Status**, it will lead to the alarm.

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

Table 14. Description of the buttons

Parameters	Function Introduction
Schedule Settings	Refer to Table 8 *(page 30)* for the meanings of the items, here will not repeat again.
Alarm Action	Refer to Table 9 *(page 31)* for the meanings of the items, here will not repeat again.

5.5.1.3 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 15. 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.

5.5.1.4 Exception

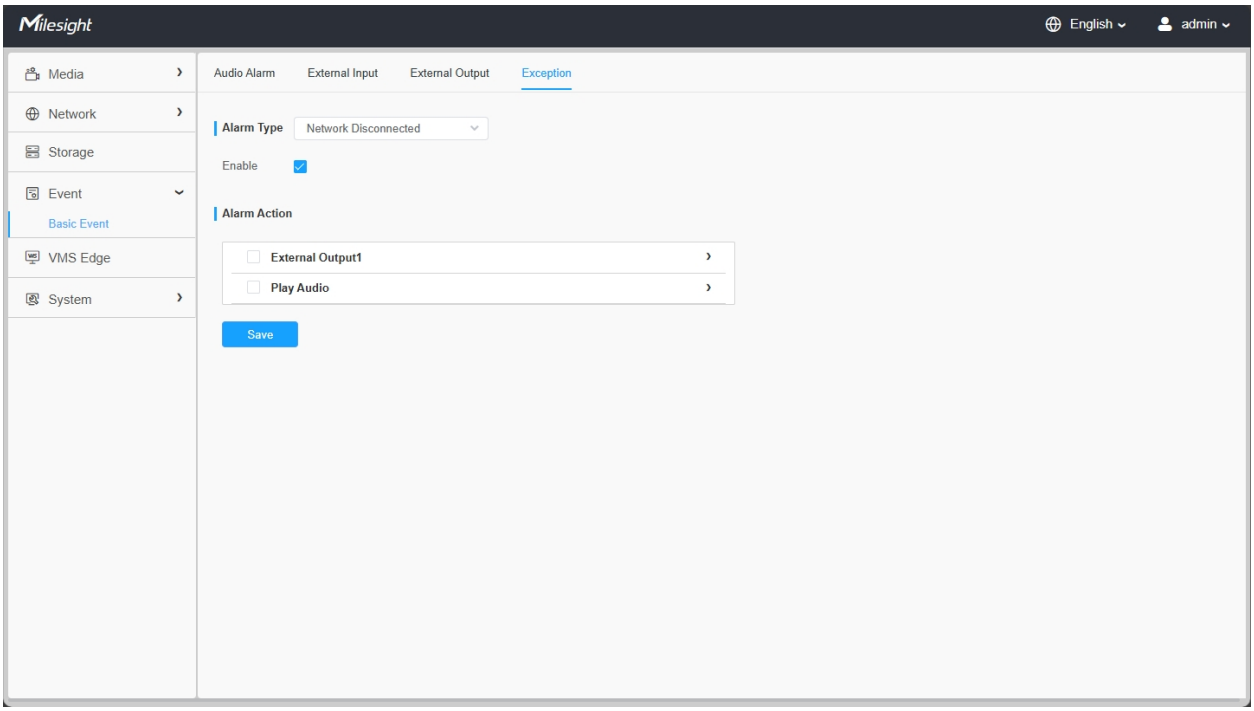
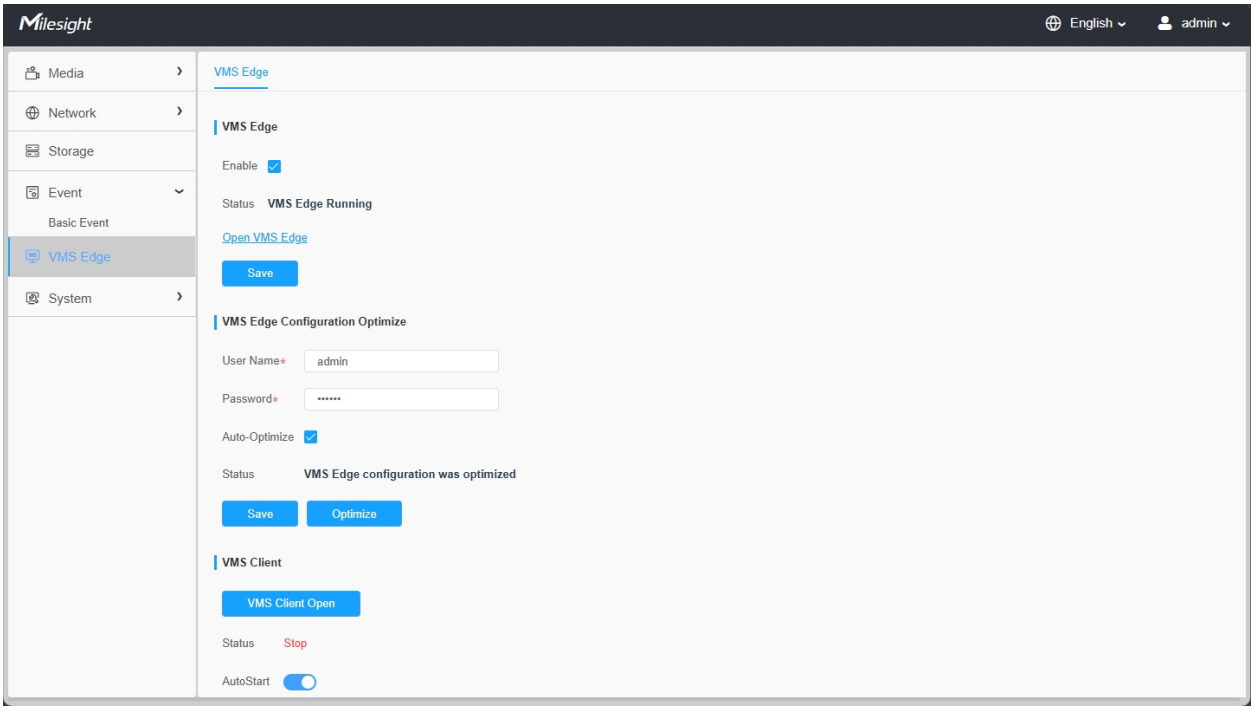


Table 16. Description of the buttons

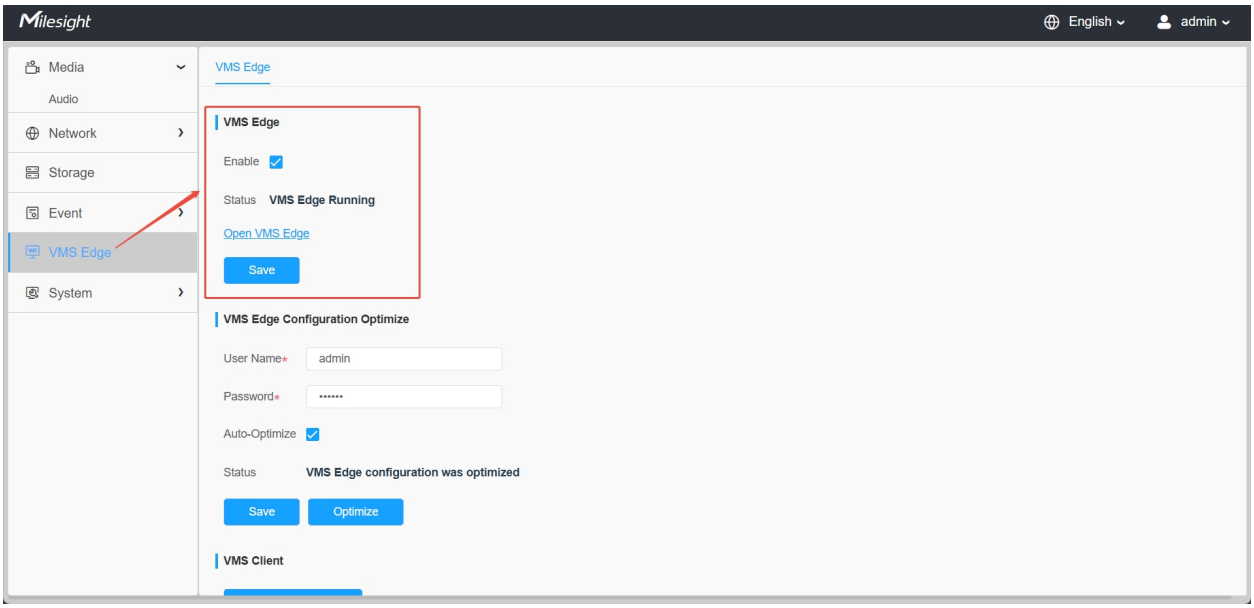
Parameters	Function Introduction
Alarm Type	**Network Disconnected**, **IP Address Conflicted**, **SSD Full**, **SSD Uninitialized**, **SSD Error**,and **No SSD** are available. Check the checkbox to enable the alarm type you selected.
Alarm Action	Refer to Table 9 *(page 31)* for the meanings of the items, here will not repeat again.

5.6 VMS Edge



VMS Edge is an auxiliary configuration and optimization tool for Nx Witness Server, specifically designed for Nx 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.

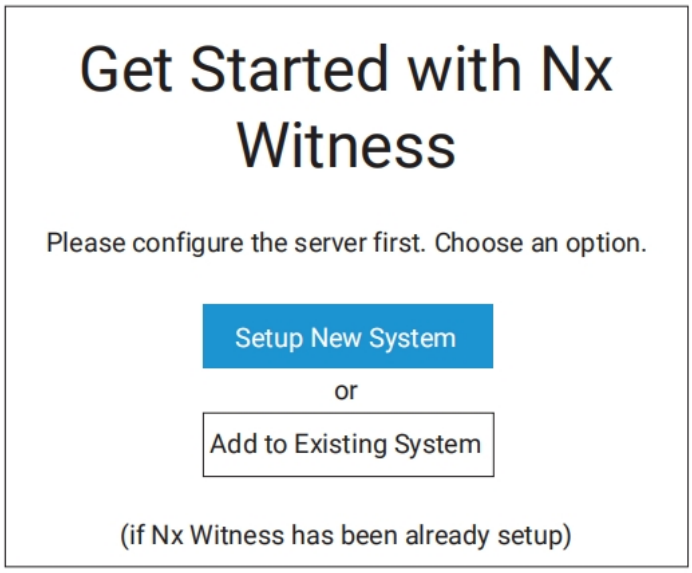
[VMS Edge]



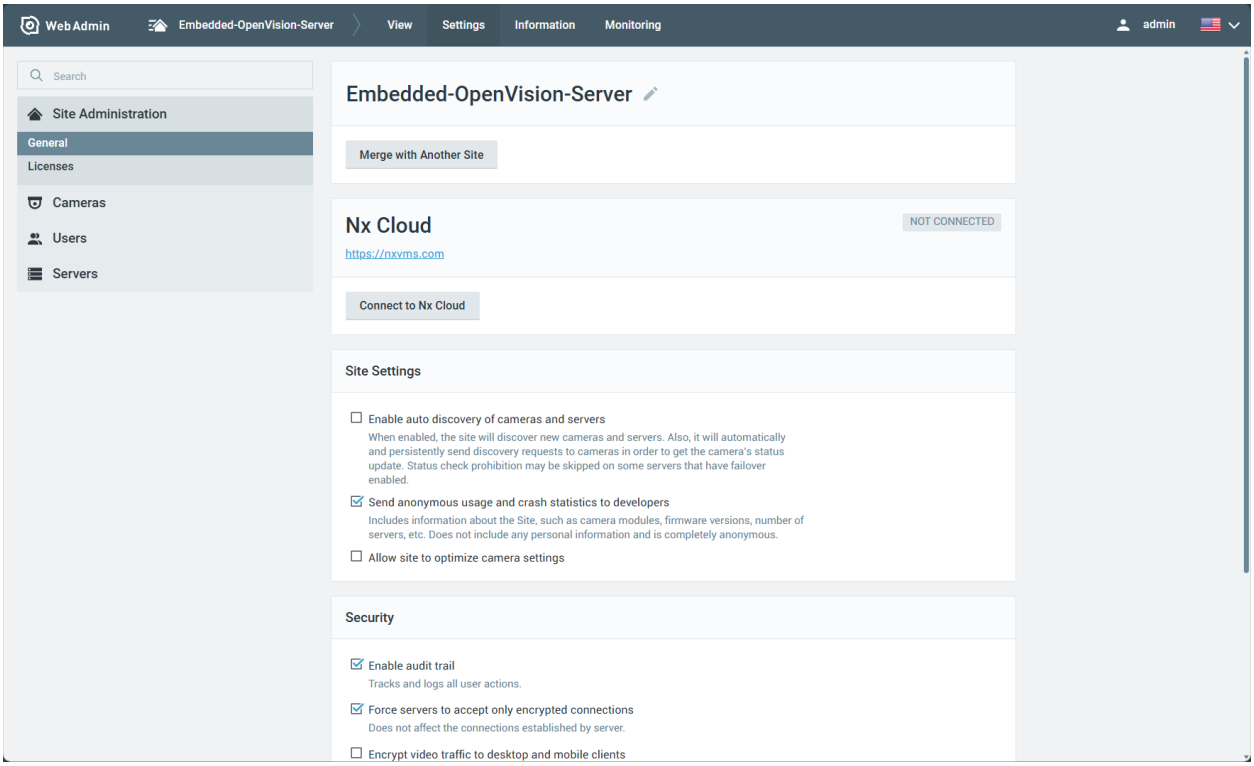
Step 1: Enable **VMS Edge** and verify whether the status shows "**VMS Edge Running**" first.

Step 2: Click Open VMS Edge to access the Nx Witness Server web page.

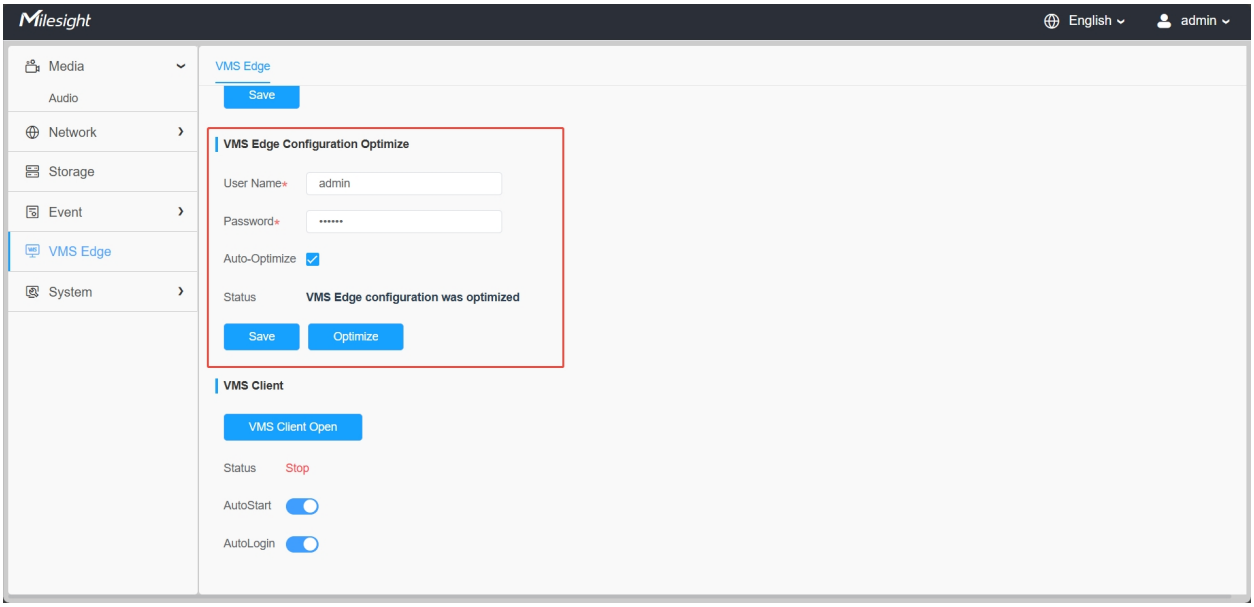
For first-time use, please click "**Setup New System**" to create a new system and complete the initialization. If a system has already been created, you can also choose to join an existing system.



After activation, you can access the WebAdmin 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.



[VMS Edge Configuration Optimize]



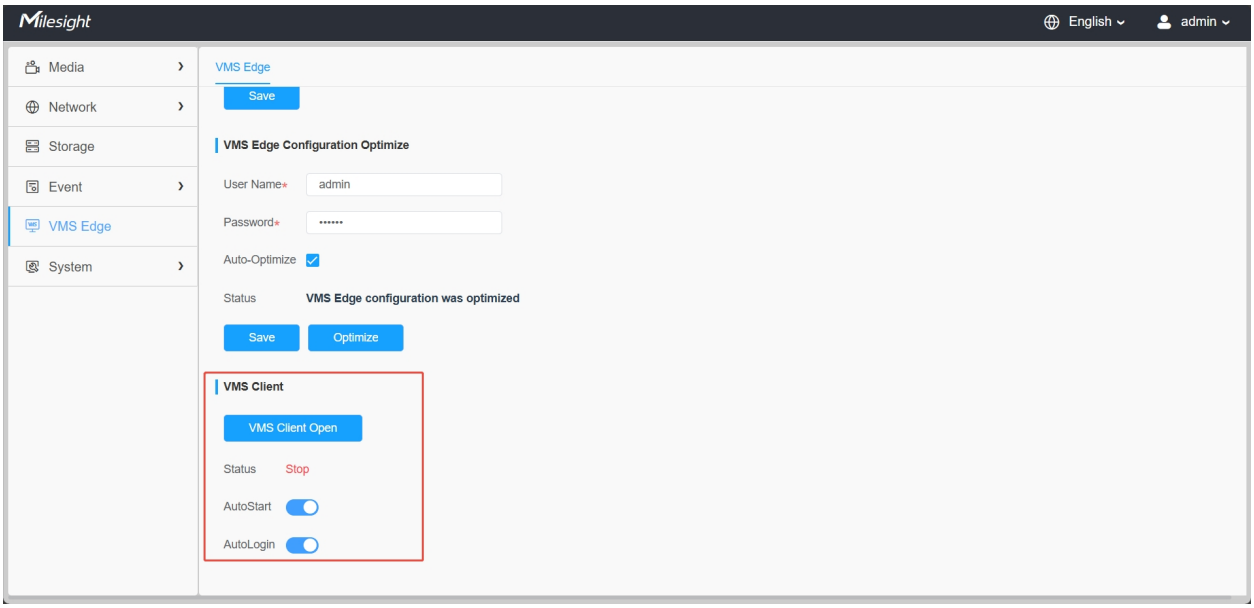
This step primarily optimizes SSD storage for optimal performance. Please ensure it is enabled, as failure to do so may result in storage errors.

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.

[VMS Client]

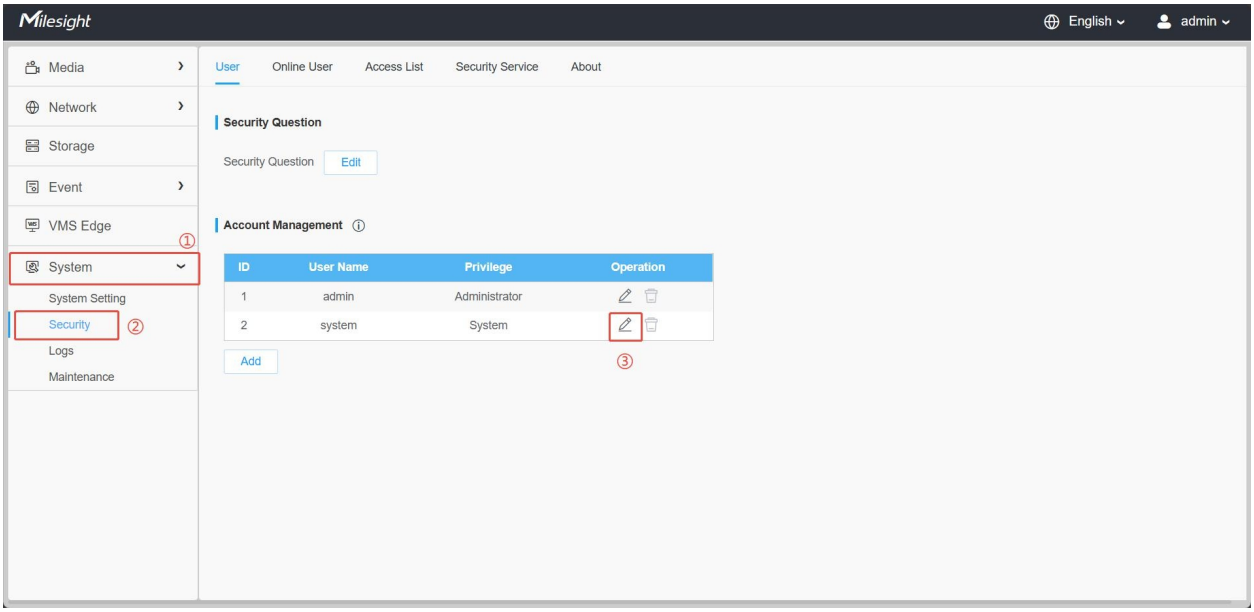


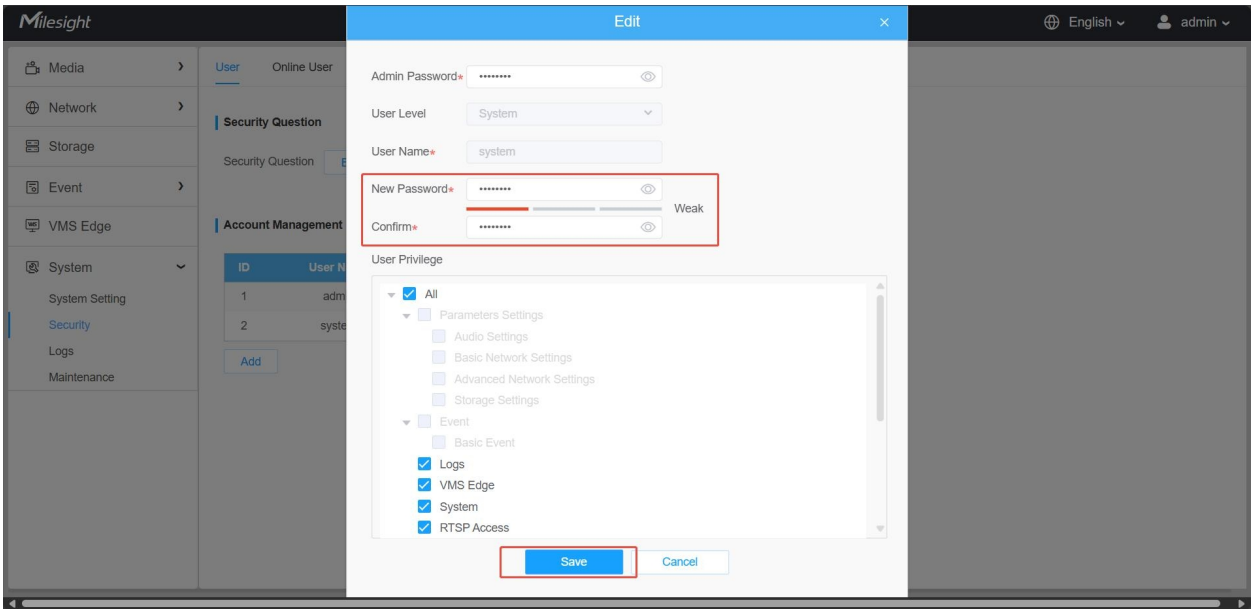
Since the device has a built-in client, users can access the Nx Witness Client directly on the connected monitor to connect to the Nx Witness Server. The steps are as follows:

Step 1: Click **System --> Security--> Edit** to modify the default password of the system account, and then save the edition.

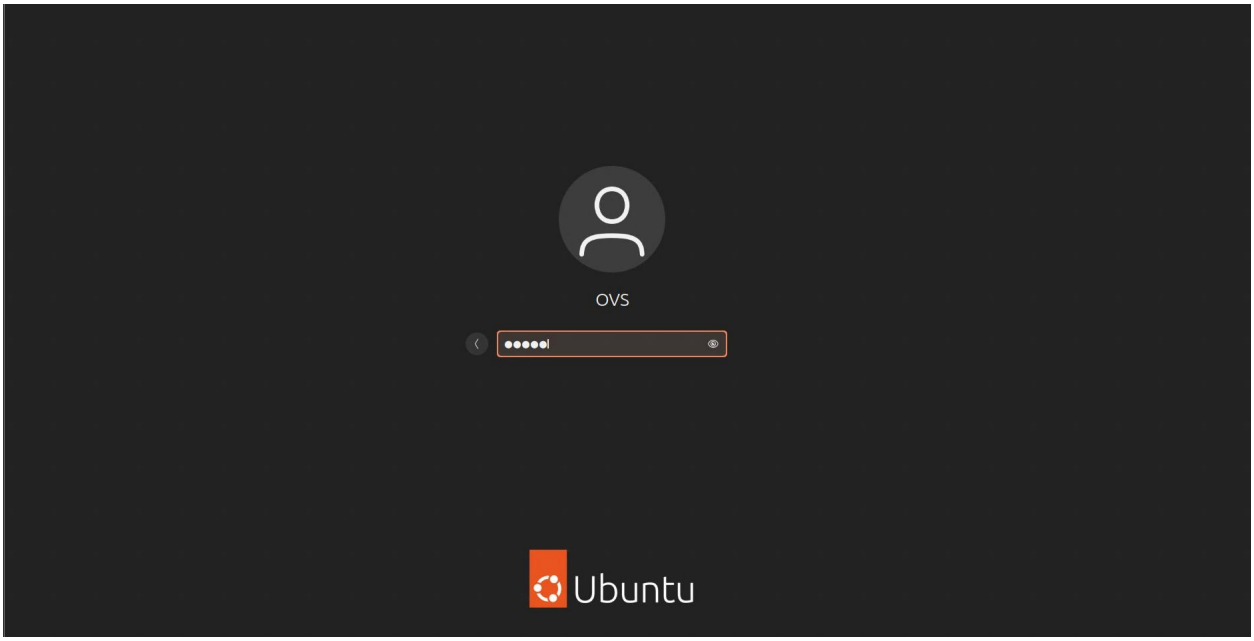
Note:

- The default password for the system user is "*admin*", which is also the Ubuntu system login password. (The Ubuntu system account's nickname is "*OVS*".) Users must set a new password before the “VMS Client” can be enabled.
- If the Ubuntu desktop password has been forgotten, it can also be reset through this step.





Step 2: Connect a display to the device using HDMI. Then, log in to the Ubuntu system using the new password.



Step 3: Click VMS Client Open on the web browser to open the Nx Witness Client on the connected display and connect to the server using the default IP address (127.0.0.1:7001) or the IP address you set during activation to complete the creation and connection of the server.

Note: Using 127.0.0.1:7001 to log in allows you to continue accessing the server even if its IP address is changed later.

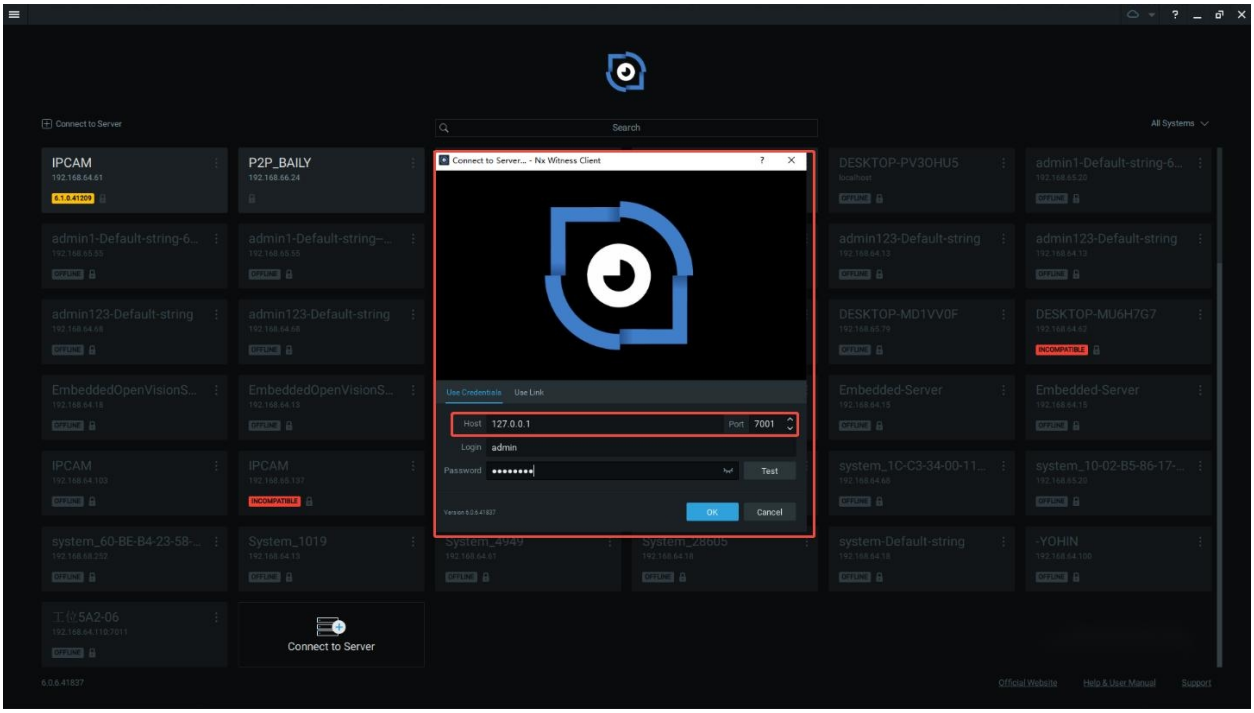


Table 17. Description of the buttons

Parameters	Function Introduction
VMS Client Open	Click to enable the Nx Witness Client and connect it to the Nx Witness Server.
AutoStart	When enabled, the Nx Witness Client will automatically start when the system boots up.
AutoLogin	For automatic login, select Remember me in the Nx Witness Client, then enable "AutoLogin" in the web interface. This way, you won't need to enter your username or password next time.

5.7 System

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

5.7.1 System Setting

Here you can check System information and Date&Time.

5.7.1.1 System Info

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

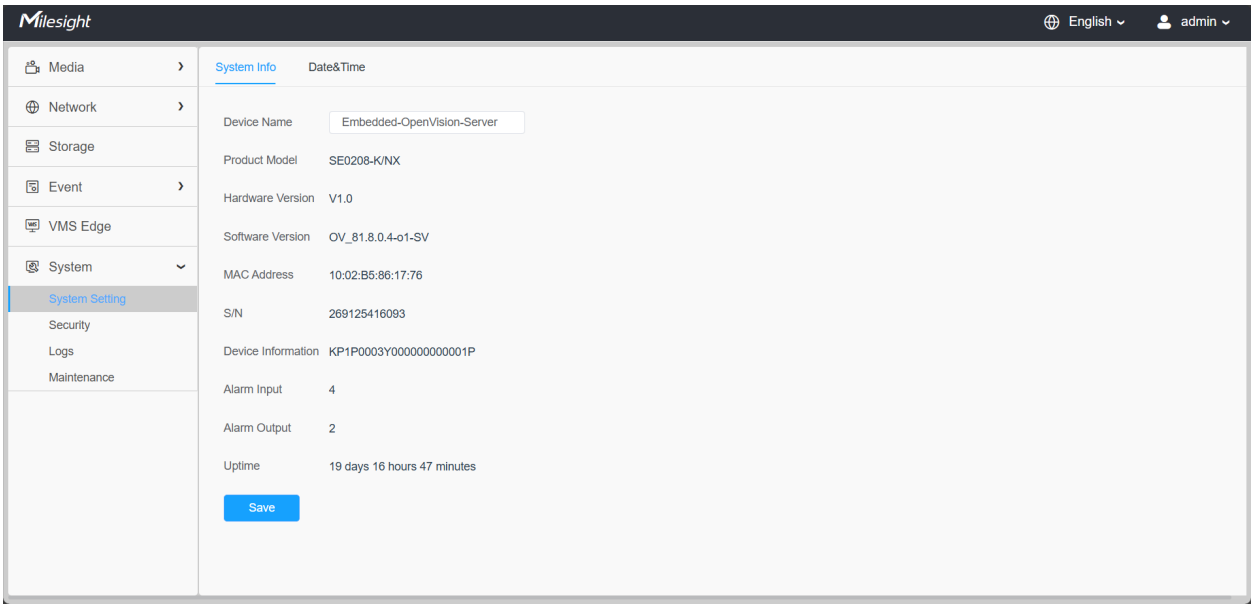


Table 18. Description of the buttons

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 software version of the device can be upgraded.
MAC Address	Media Access Control address.
S/N	Stock Number.
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.

Parameters	Function Introduction
Save	Save the configuration.

5.7.1.2 Date&Time

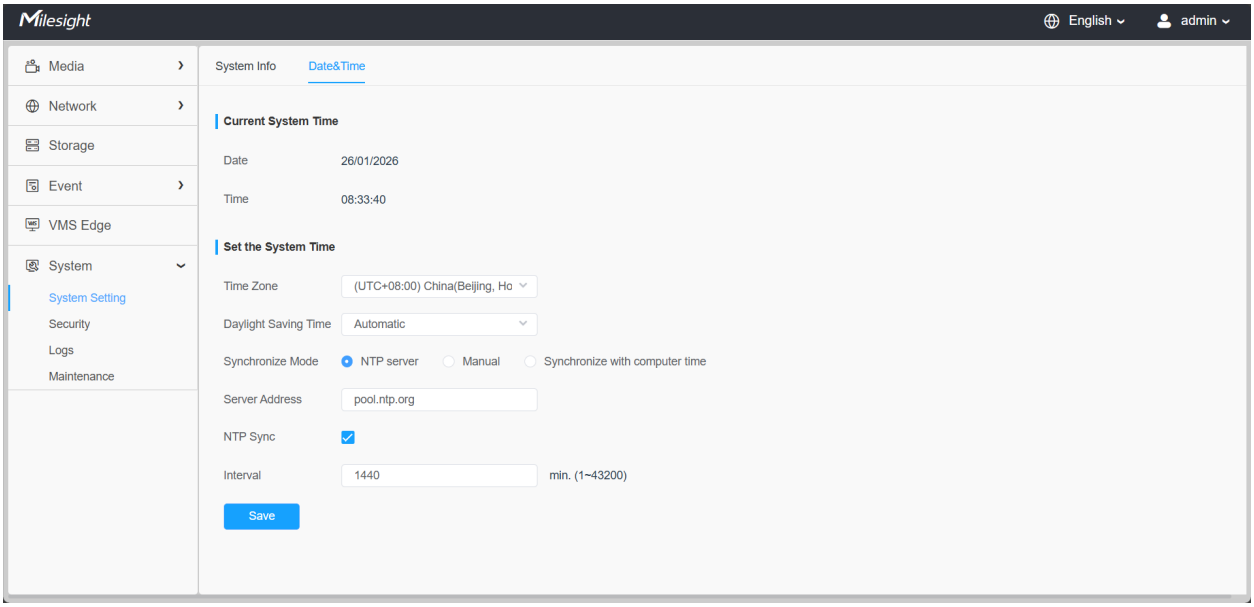


Table 19. Description of the buttons

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.

5.7.2 Security

Here you can configure User, Access List, Security Service, etc.

5.7.2.1 User

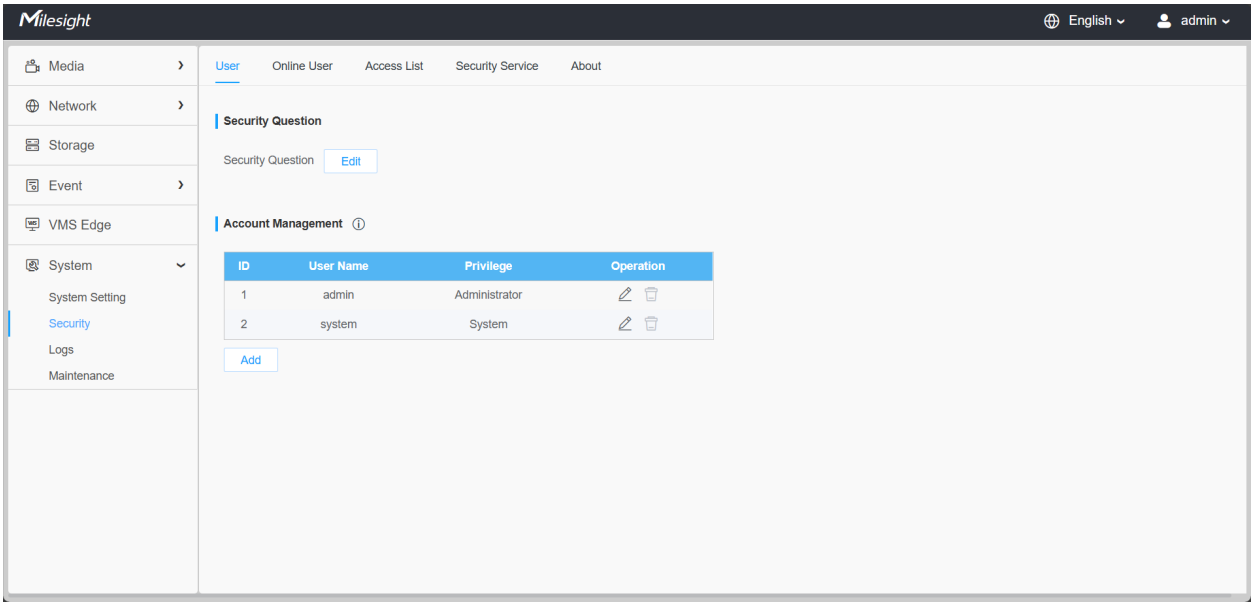
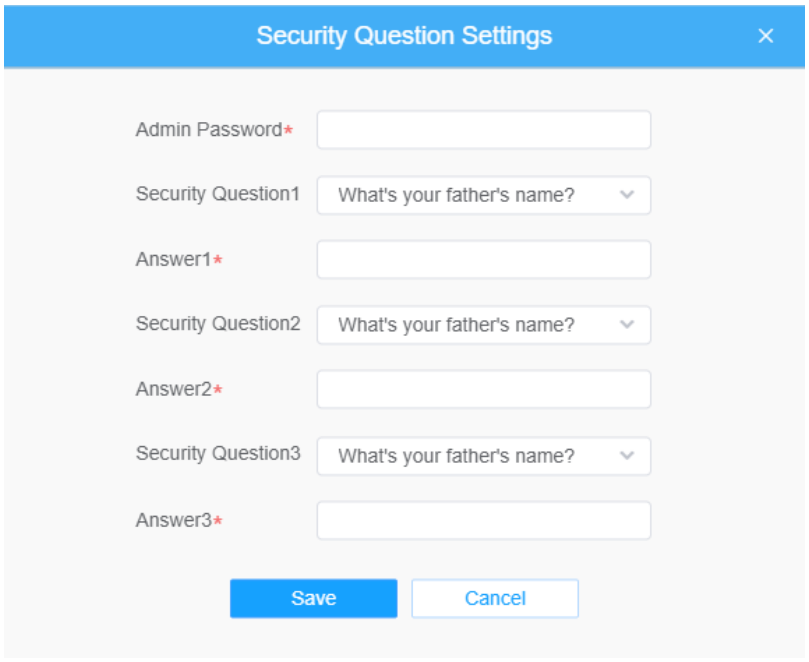
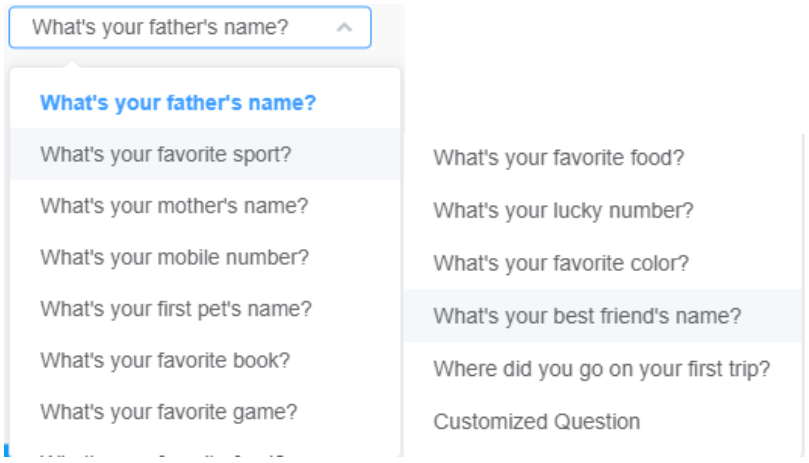
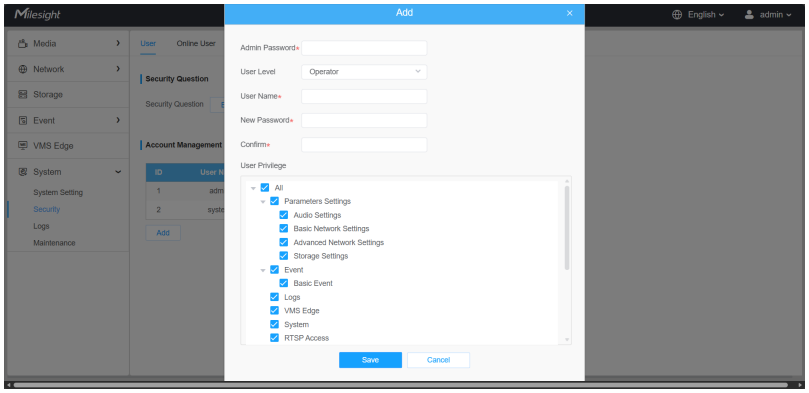
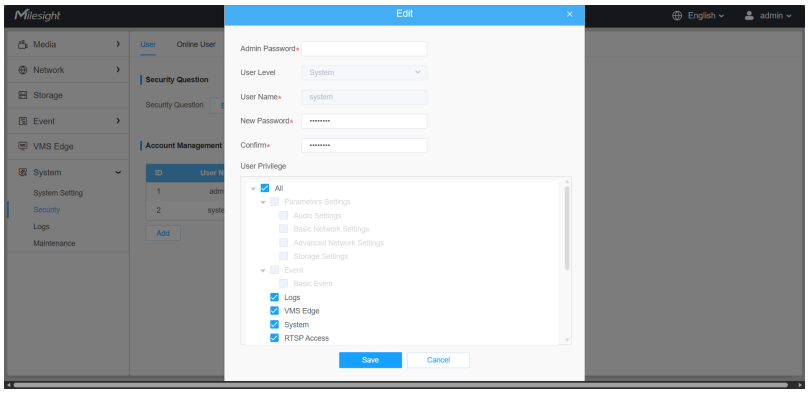


Table 20. Description of the buttons

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.

5.7.2.2 Online User

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

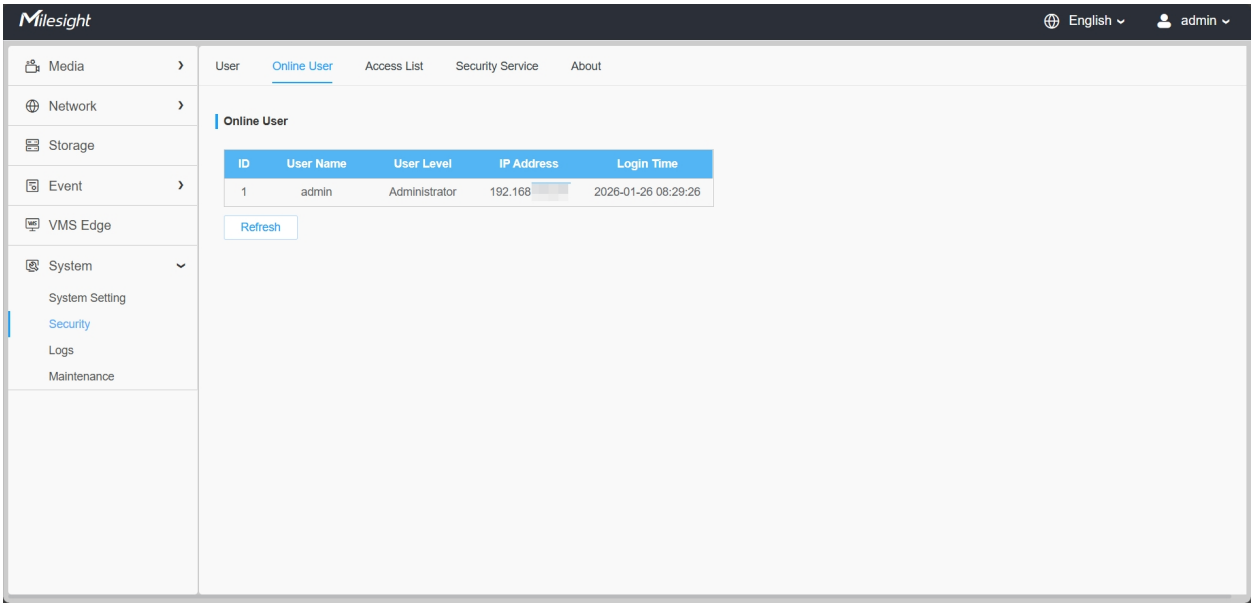


Table 21. Description of the buttons

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.

5.7.2.3 Access List

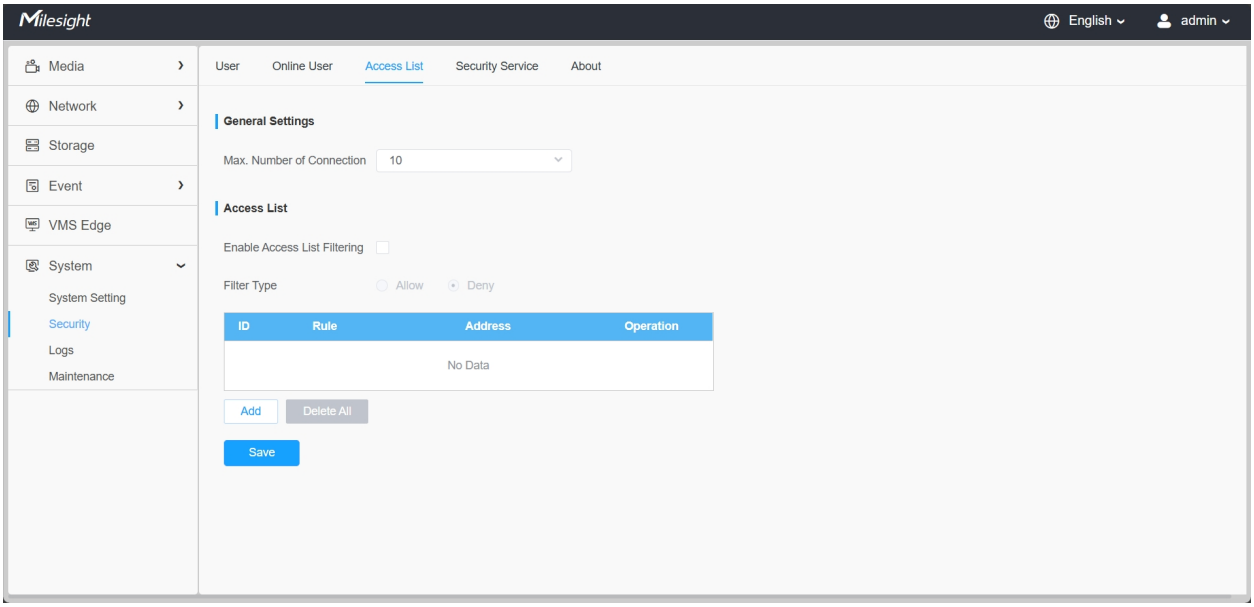
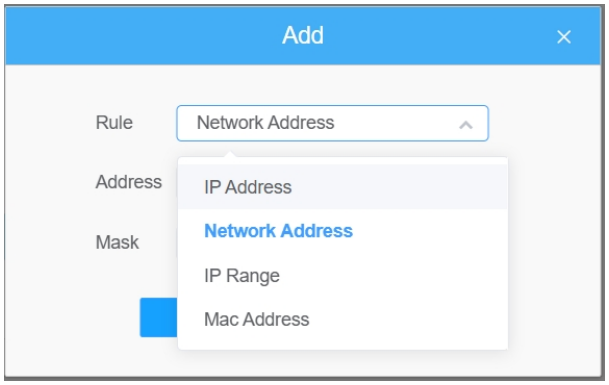


Table 22. Description of the buttons

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.

<table>
<tr><th>Parameters</th><th colspan="2">Function Introduction</th></tr>
<tr><td rowspan="4"></td><td>Add</td><td> 

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 get the access to the device. You also need to set the Mask value to finish the addition (valid range: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.</td></tr>
<tr><td>Delete All</td><td>Delete all the access list.</td></tr>
<tr><td></td><td>Edit the selected IP on access list.</td></tr>
<tr><td></td><td>Delete the selected IP on access list.</td></tr>
<tr><td>Save</td><td colspan="2">Save the configuration.</td></tr>
</table>

5.7.2.4 Security Service

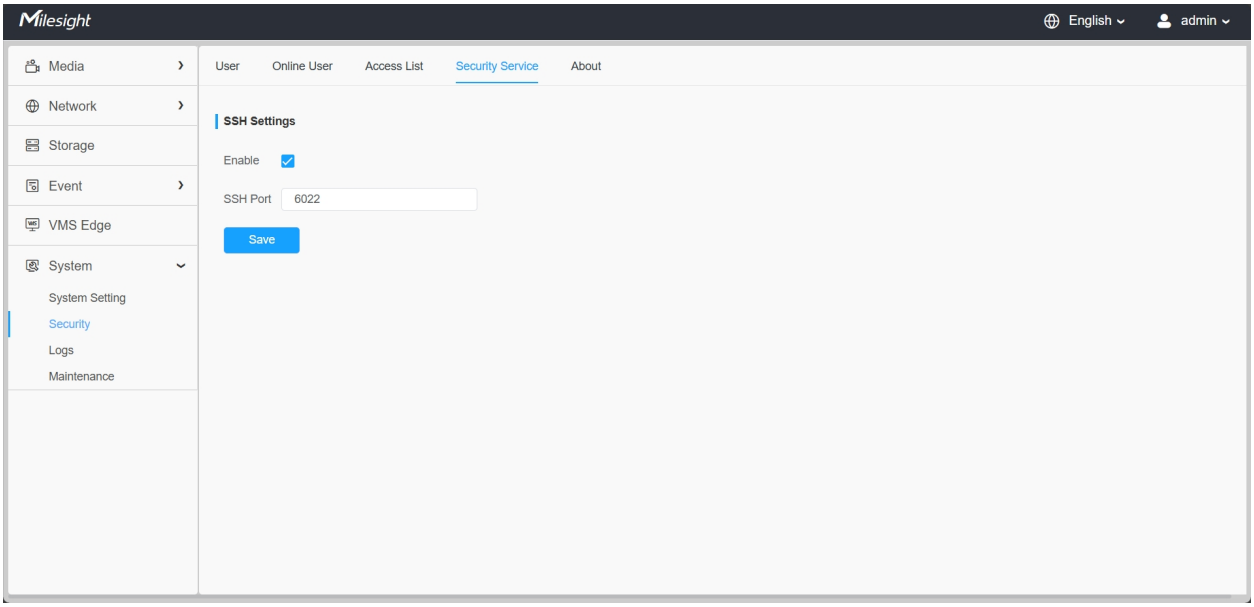
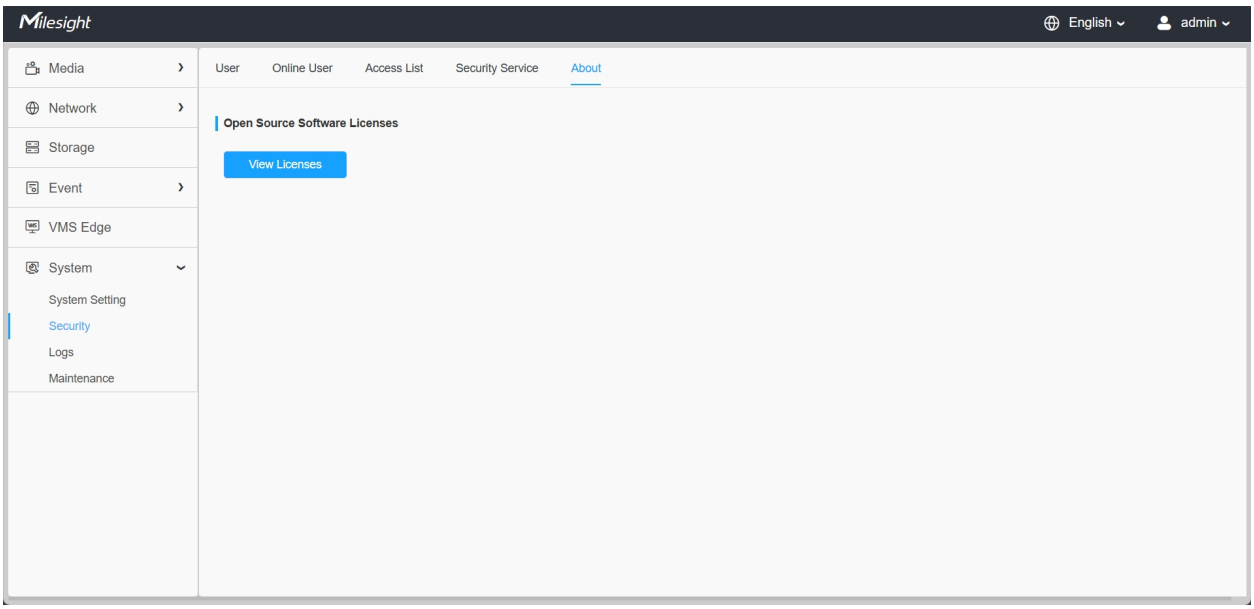


Table 23. Description of the buttons

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.

5.7.2.5 About



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

5.7.3 Logs

The logs contain the information about the time and IP that has accessed the device through web.

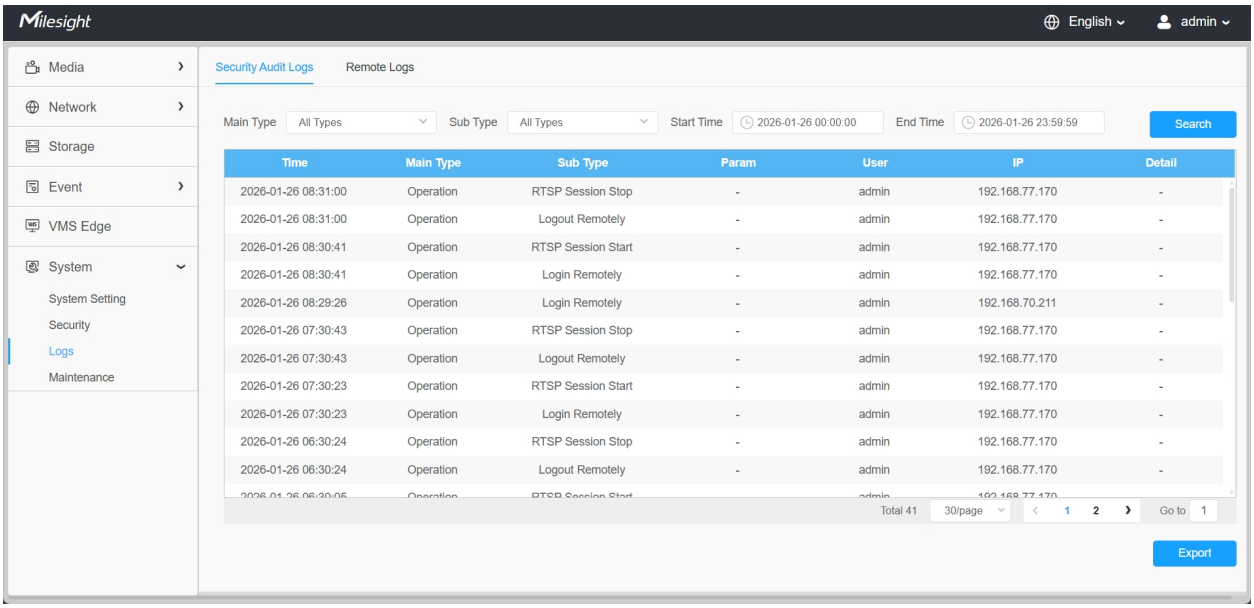


Table 24. Description of the buttons

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	Search the logs.
Export	Export the logs.

Parameters	Function Introduction
Go to	Input the number of logs' page.

5.7.4 Maintenance

Here you can configure System Maintenance and Auto Reboot.

5.7.4.1 System Maintenance

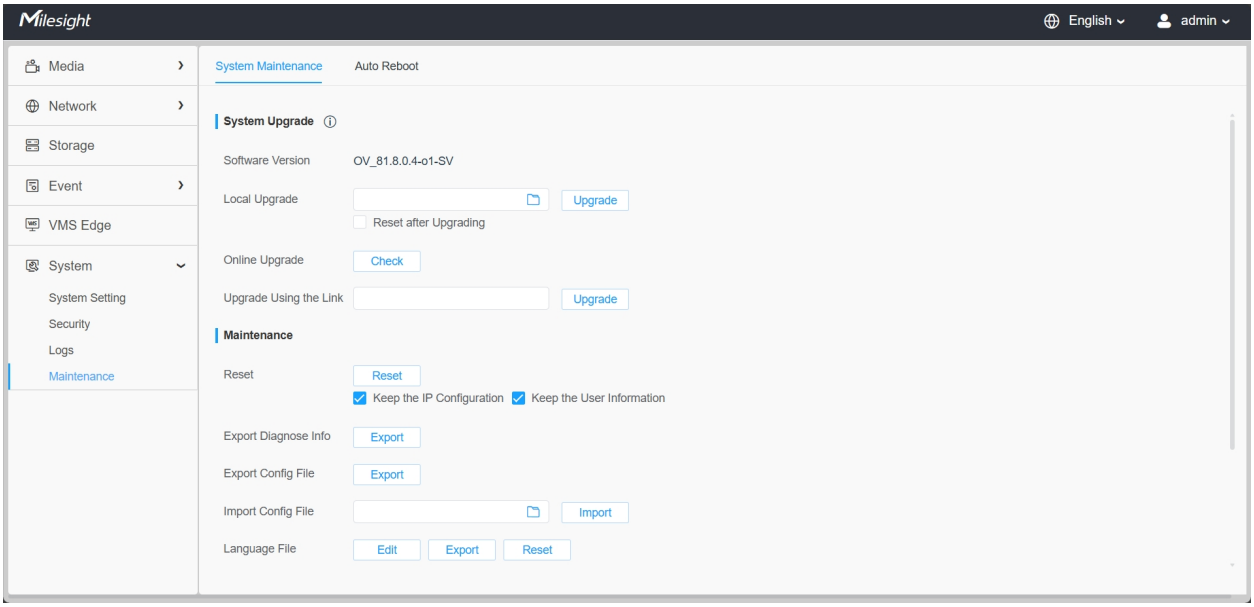
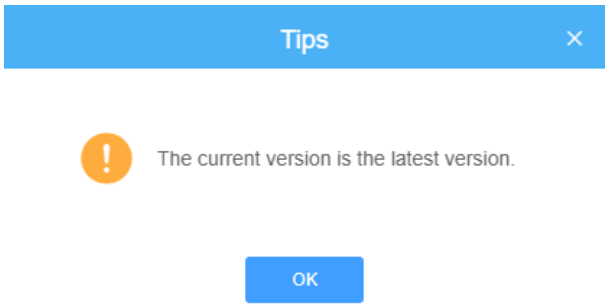
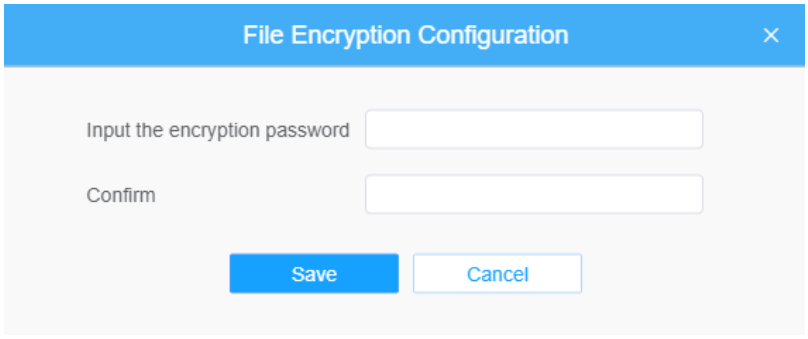
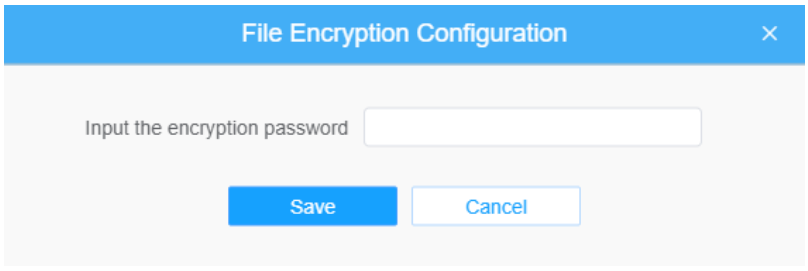


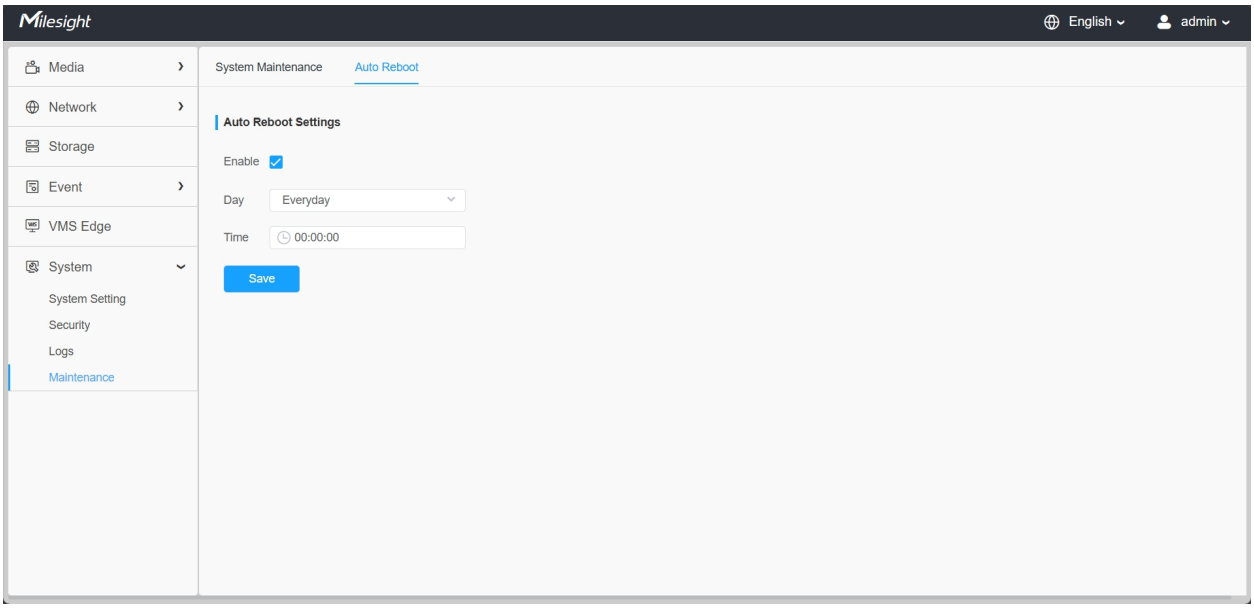
Table 25. Description of the buttons

Parameters	Function Introduction
System Upgrade	**Software Version:** The software version of the camera. **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 firmware version on our website, and then click "OK" to upgrade to this version. It will prompt "The current version is the latest version" 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.

Parameters	Function Introduction
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.  **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.

Parameters	Function Introduction
Reboot	Click “Reboot” button to restart the device immediately.

5.7.4.2 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.

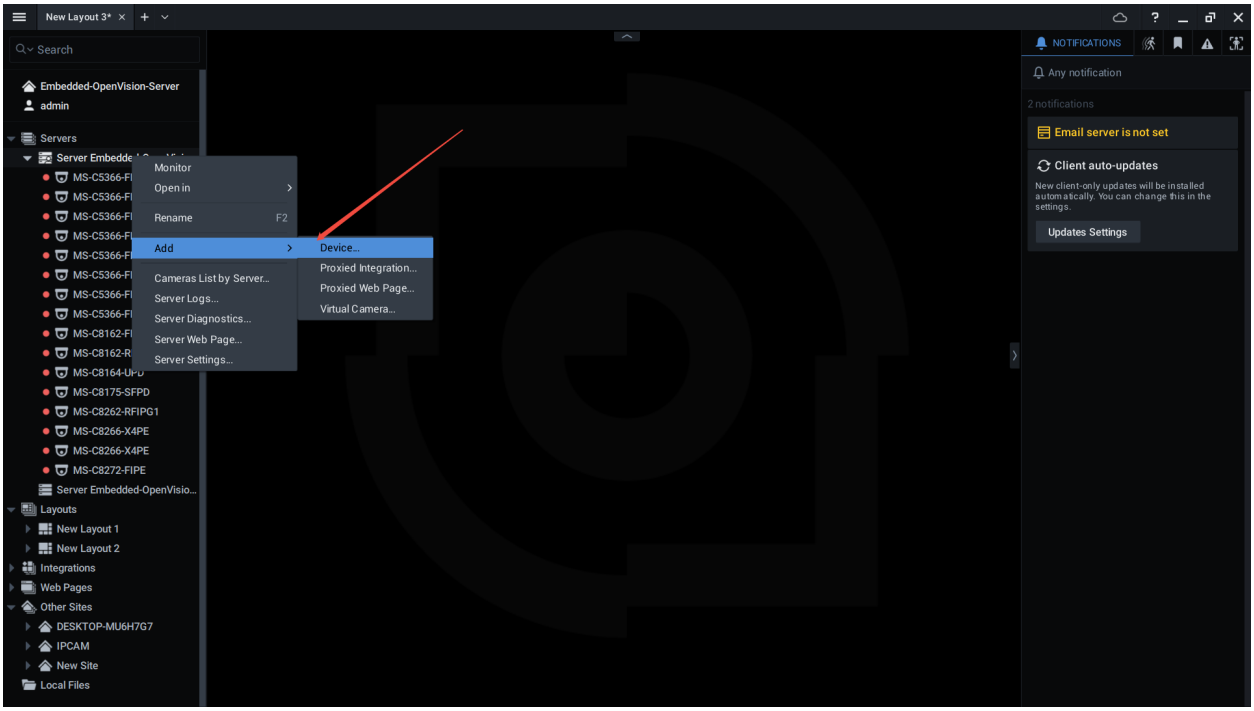
Chapter 6. Integration with NX Server

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 5.6 VMS Edge *(page 37)*.

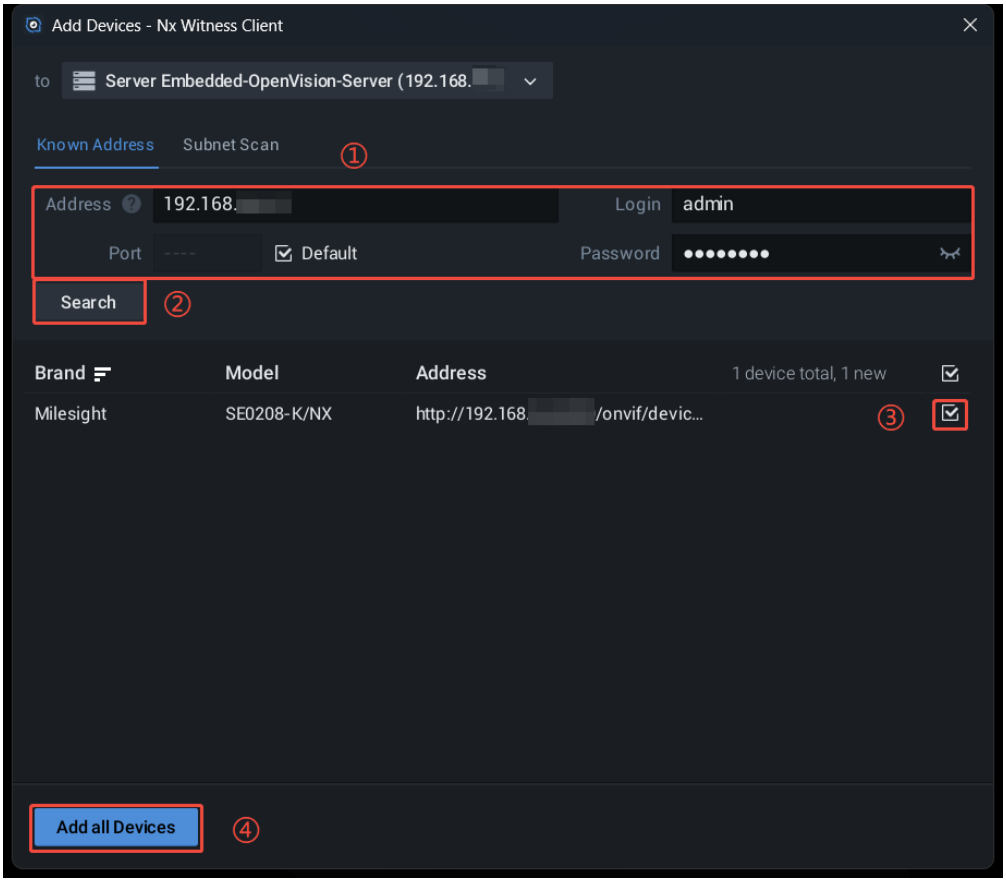
6.1 Add Device

Milesight OpenVision Server Mini can be integrated into Nx 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.



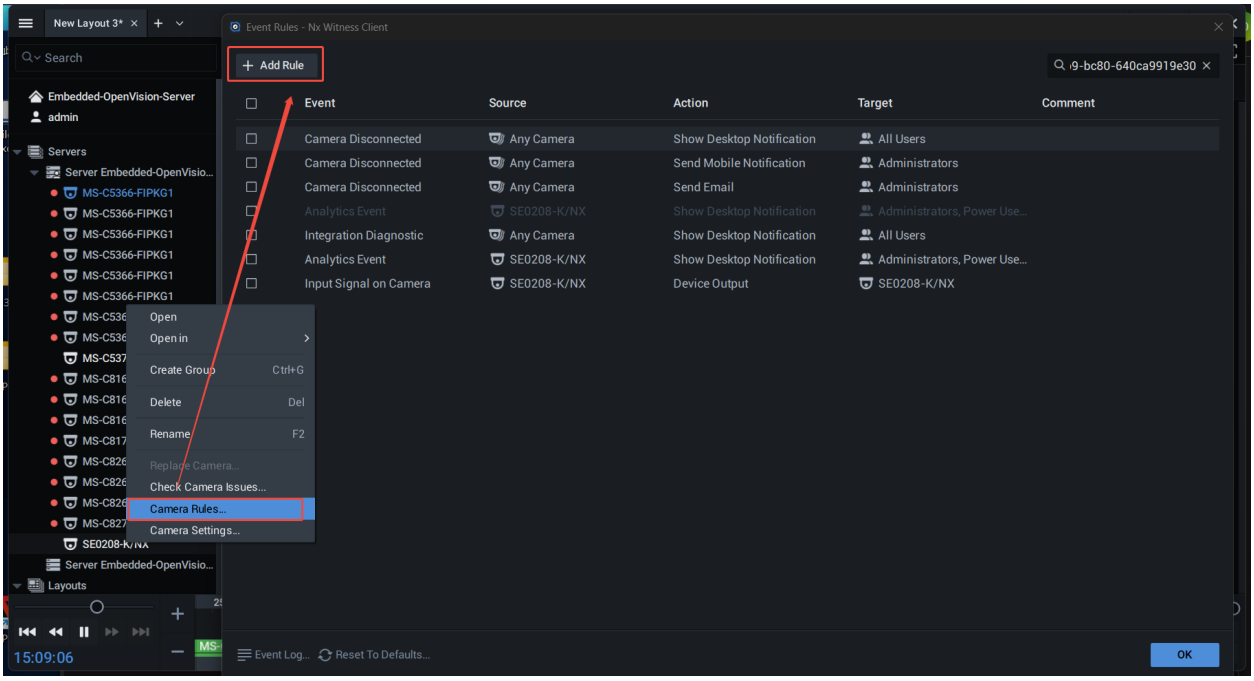
Step 2: Enter the device's IP address, username, and password, then click "**Search**". Once the device is found, check the box next to it and click "**Add all Device**" to add it.



6.2 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:**

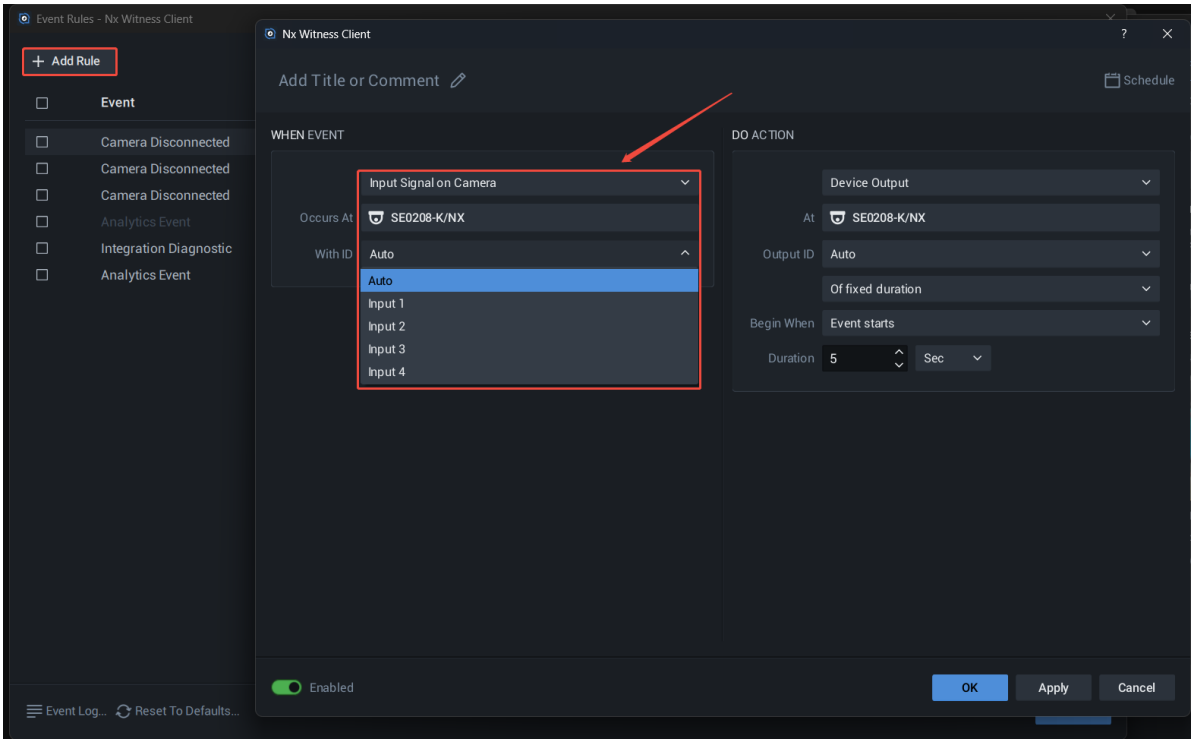


Table 26. Description of Fields

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:**

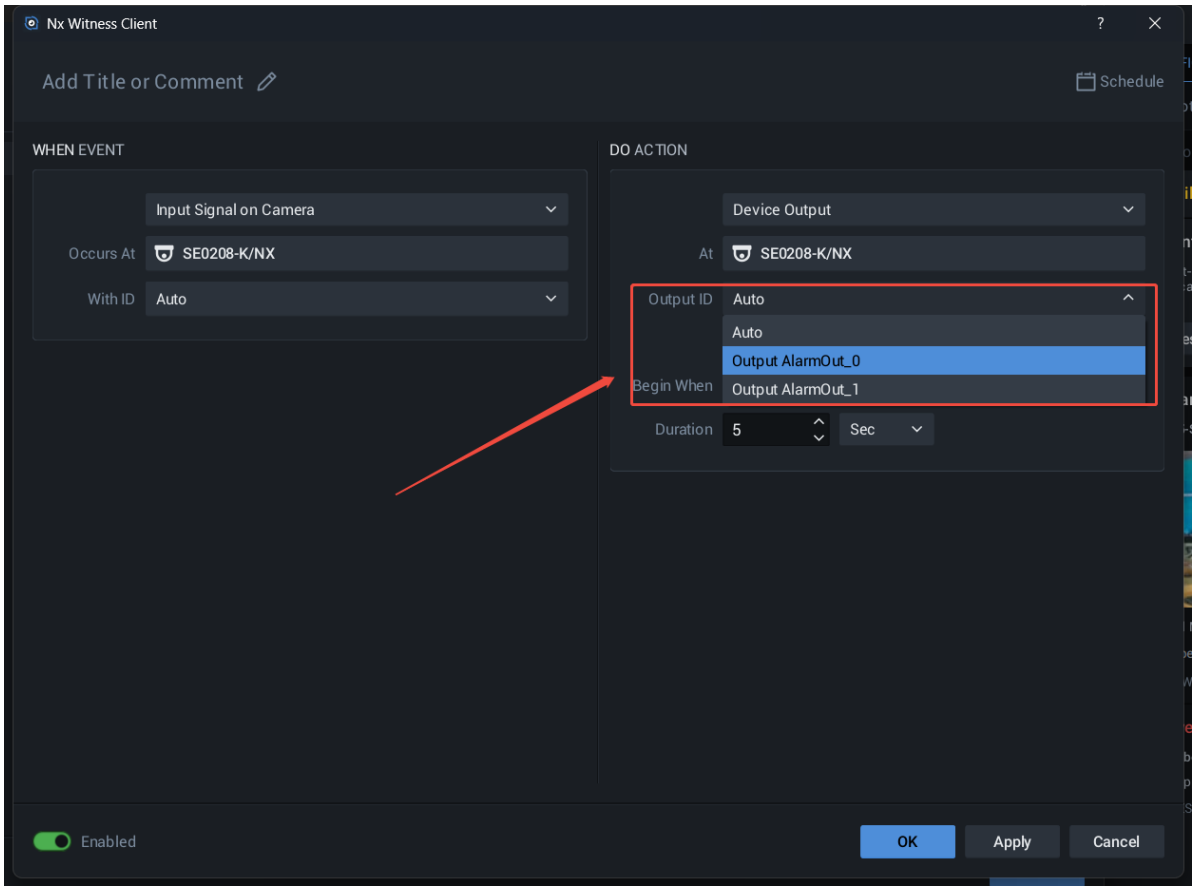
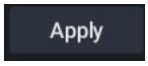


Table 27. Description of Fields

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

Parameters	Function Introduction
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: ◦ **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. ◦ **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.

6.3 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.

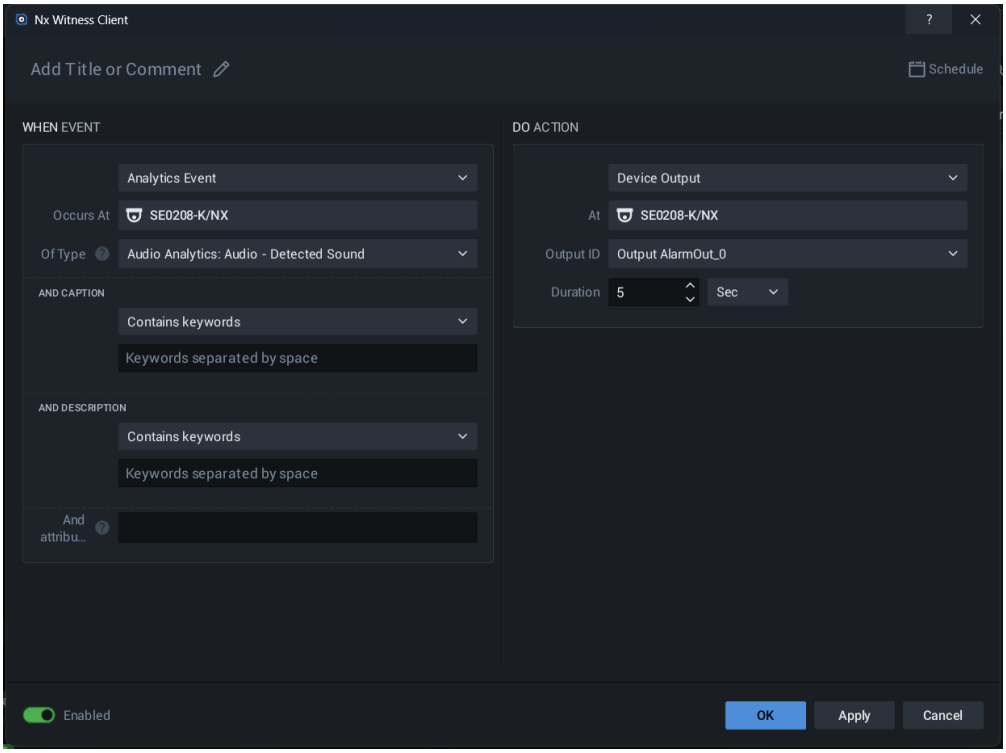


Table 28. Description of Event Fields

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.

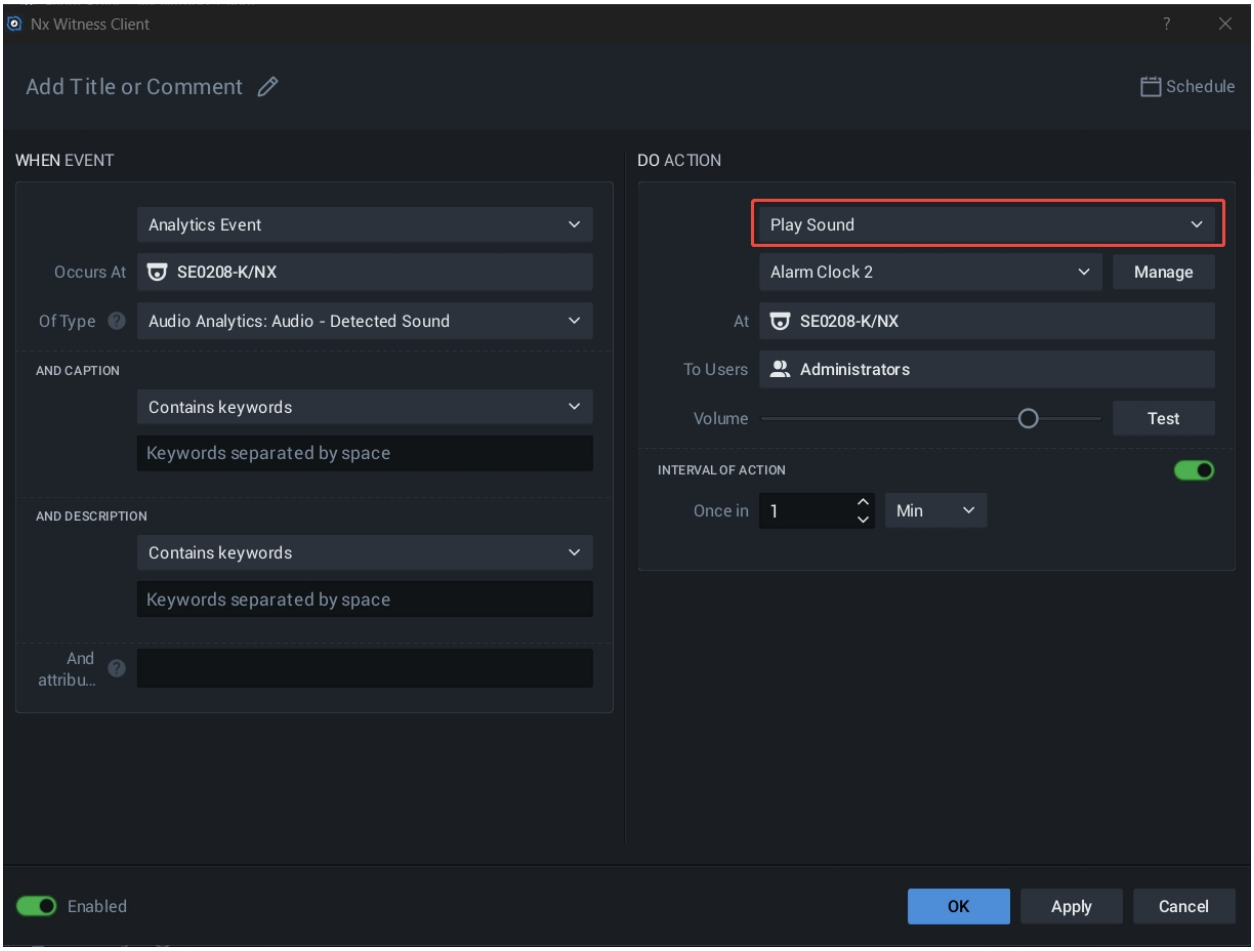
Parameters	Function Introduction
AND attribute	A text field where users can input specific attributes. The event will be triggered only if the event matches the specified attribute(s).

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

6.4 Play Sound

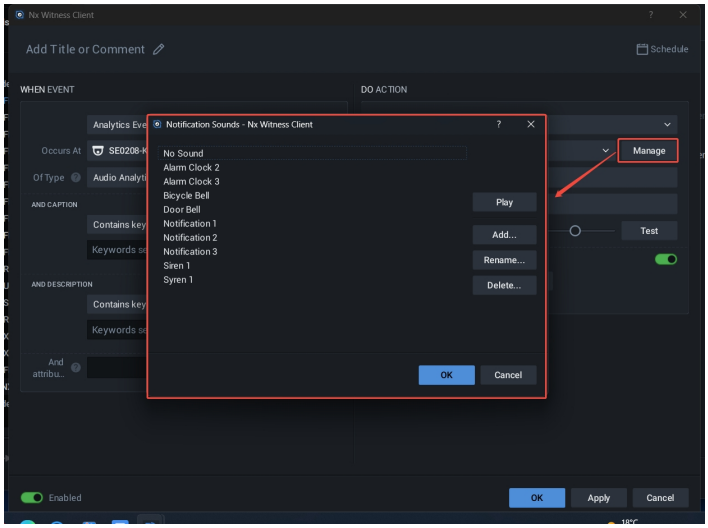
Step 1: Right-click the device and choose "Camera Rules". Then click "Add Rule" in the pop-up window.

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



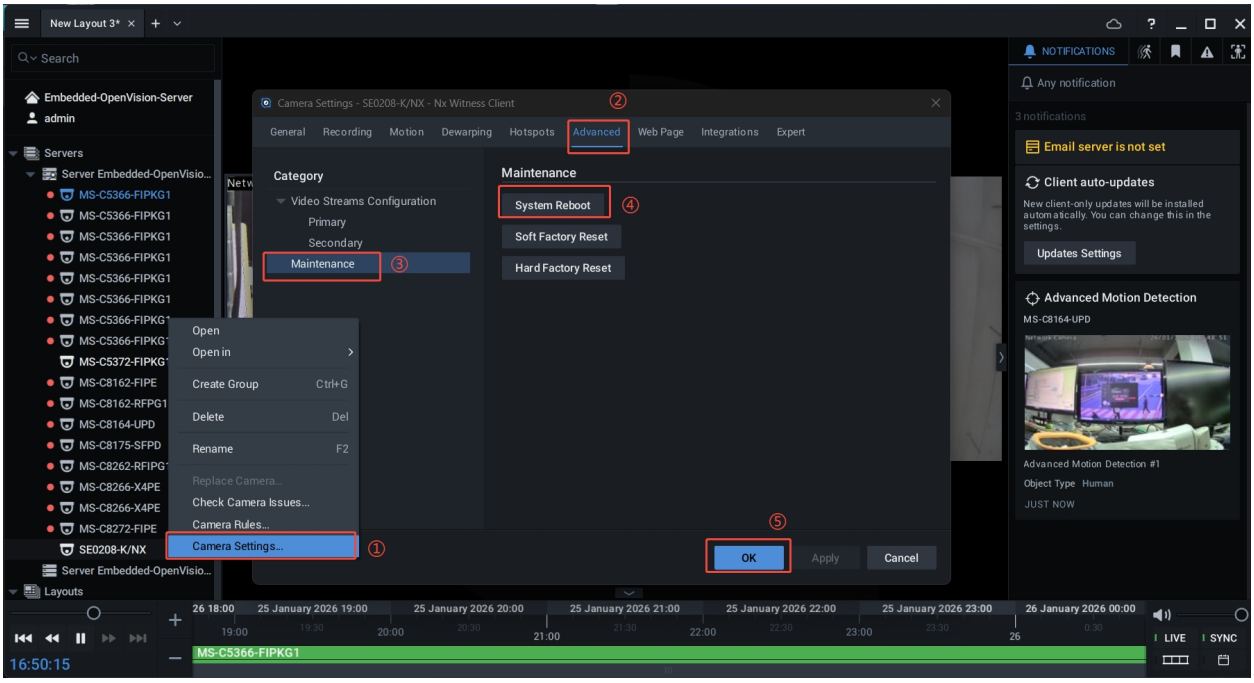
For details on the Event section fields, please refer to Table 24 *(page 60)*. Here will not repeat again.

Table 29. 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.

6.5 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.

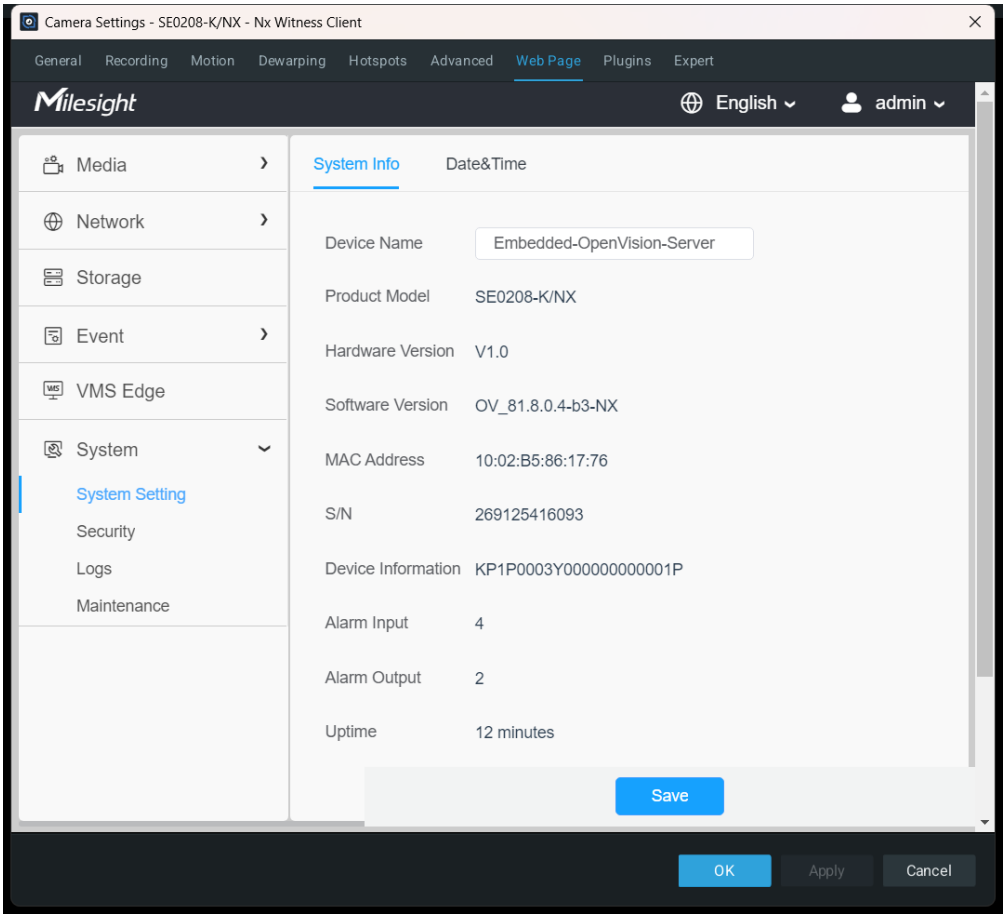
Step 5 : Click **"OK"**.

6.6 Web Page

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

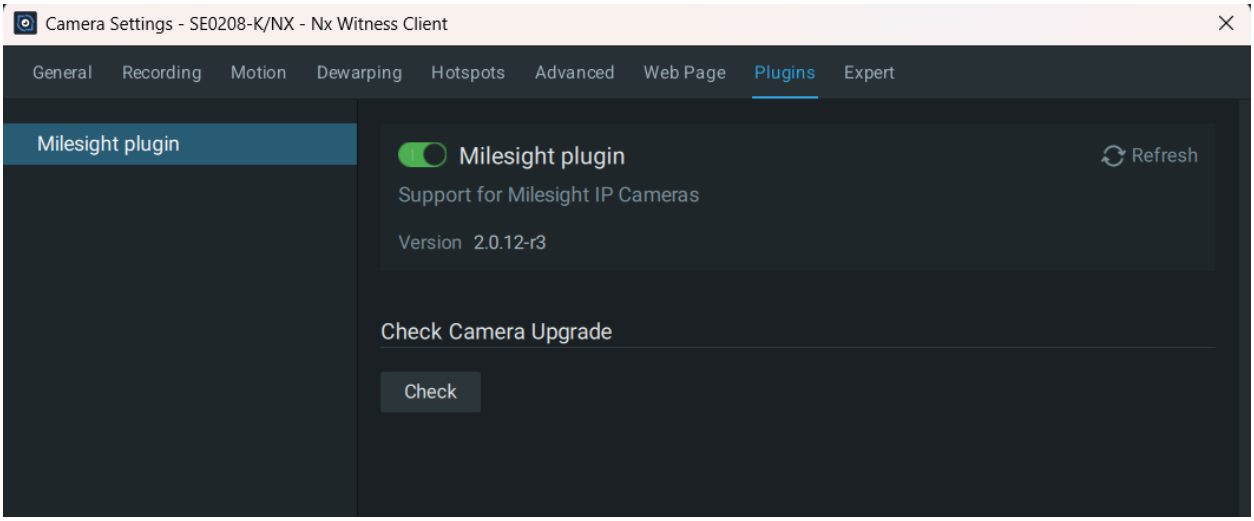
This feature allows users to directly open the device's built-in web page for advanced configuration, or accessing features not available in the Nx Witness Client. By accessing the web interface, users can manage firmware updates, network settings, user accounts, or other functions.

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



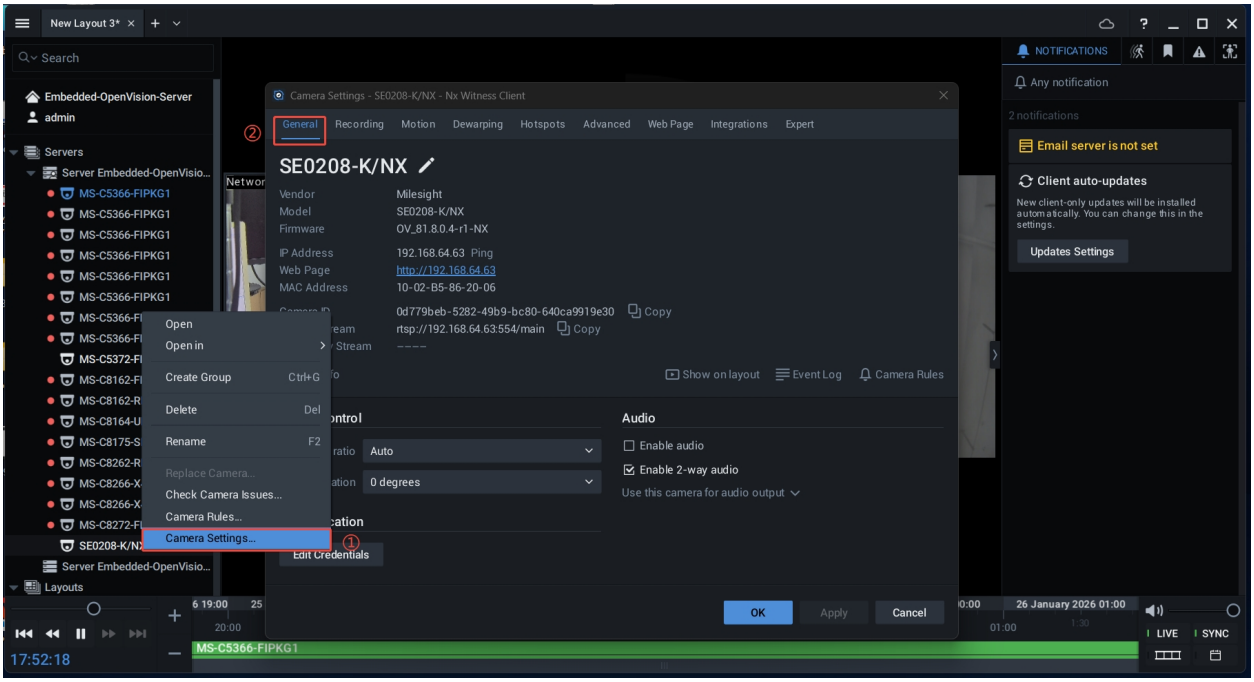
6.7 Firmware Upgrade

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

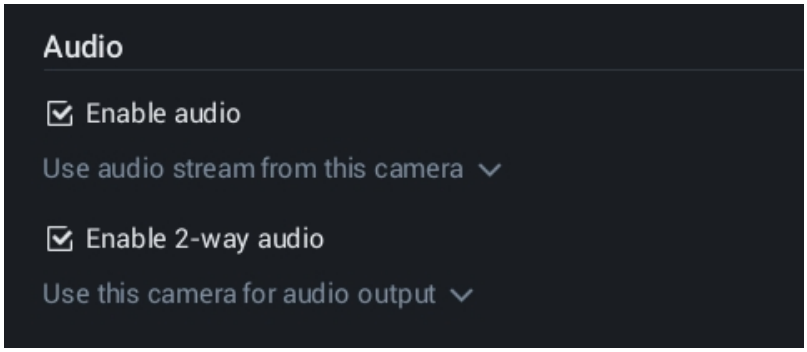


6.8 Device Info

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 7. 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.

7.1 General Configuration

7.1.1 Ubuntu Login

Two users will be pre-configured:

- A **root** user:

  Please contact our technical support to obtain the password for this account.

- A **system** user:

  The System user is used to log in to the Ubuntu desktop and run the Nx Witness Client (without root privileges or sudo privileges). The default password is **admin**, and it can be configured and changed via the web interface.

7.1.2 Device Activation

There will be activation for both the web management interface and the Nx Server.

- **Web Management activation:** For detailed steps, please refer to 4.1 Assigning an IP Address Using Smart Tools *(page 11)*.

- **Nx Server activation:** like other Nx services, can be performed via the Nx Witness Client or by activating through the web interface using the device's IP address. For detailed steps, please refer to 5.6 VMS Edge *(page 33)*.

7.2 Common Issues

7.2.1 IP Conflicts

How to Handle IP Conflicts (Smart Tools Search IP is Different from Ubuntu IP)?

It is recommended to upgrade the firmware first. If you are unable to connect to the device, you can delete the redundant network configurations in the Ubuntu interface.

7.2.2 Server Inaccessibility

How to Handle Server Inaccessibility?

It is recommended to upgrade the firmware first. If the issue persists after upgrading the firmware, you need to format the SSD via the web interface.

Note: Do not format the SSD via the Ubuntu desktop! The SSD must be formatted via the web interface!!

7.2.3 Webpage Crash

How to Handle Webpage Crash?

It is recommended to upgrade the firmware first.

7.2.4 Device Reset

How to reset the device?

There are two methods for you to reset the device.

Method 1: Physical Reset

By Pressing the physical button (the RESET button) on the device.

- **Hard Factory Reset:**

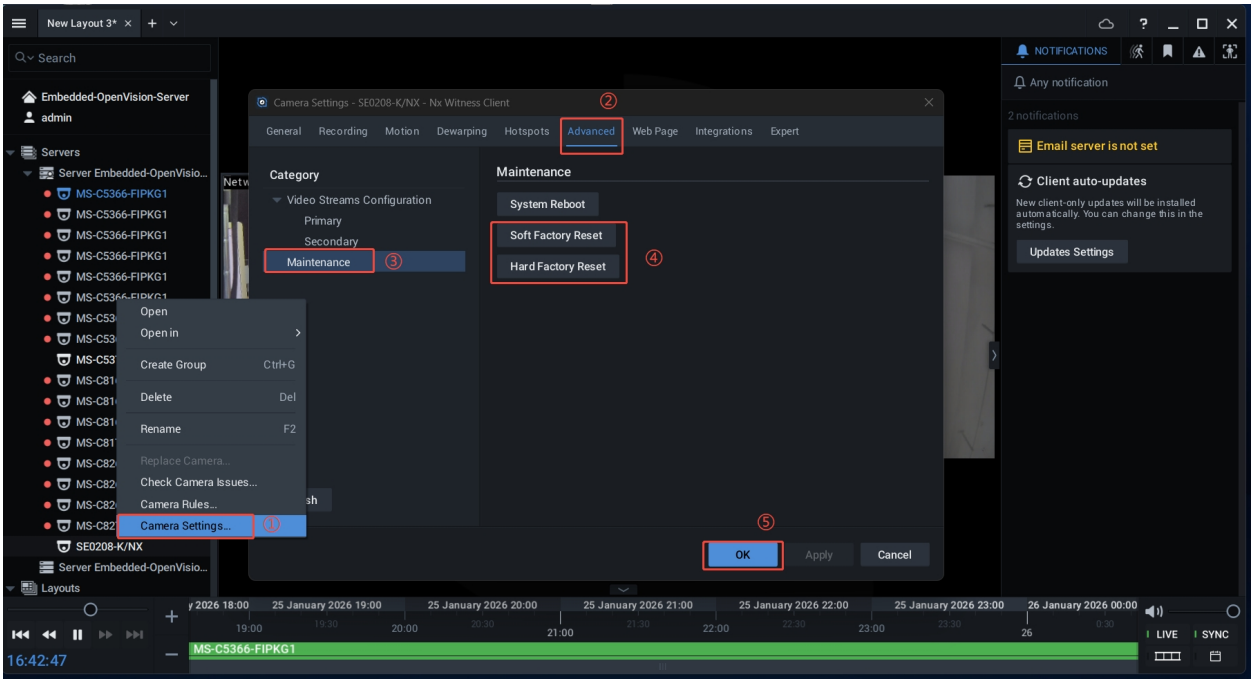
  With the device powered off, press and hold the Reset button. While holding the button, power on the device and continue holding for 10 seconds, then release to perform a factory reset. This operation will **erase the IP address, user information, and Nx Server configuration**.

- **Soft Factory Reset:**

While the device is powered on, press and hold the physical Reset button for more than 10 seconds to perform a soft reset. This operation restores factory settings **without erasing the IP address, user information and Nx Server configuration**.

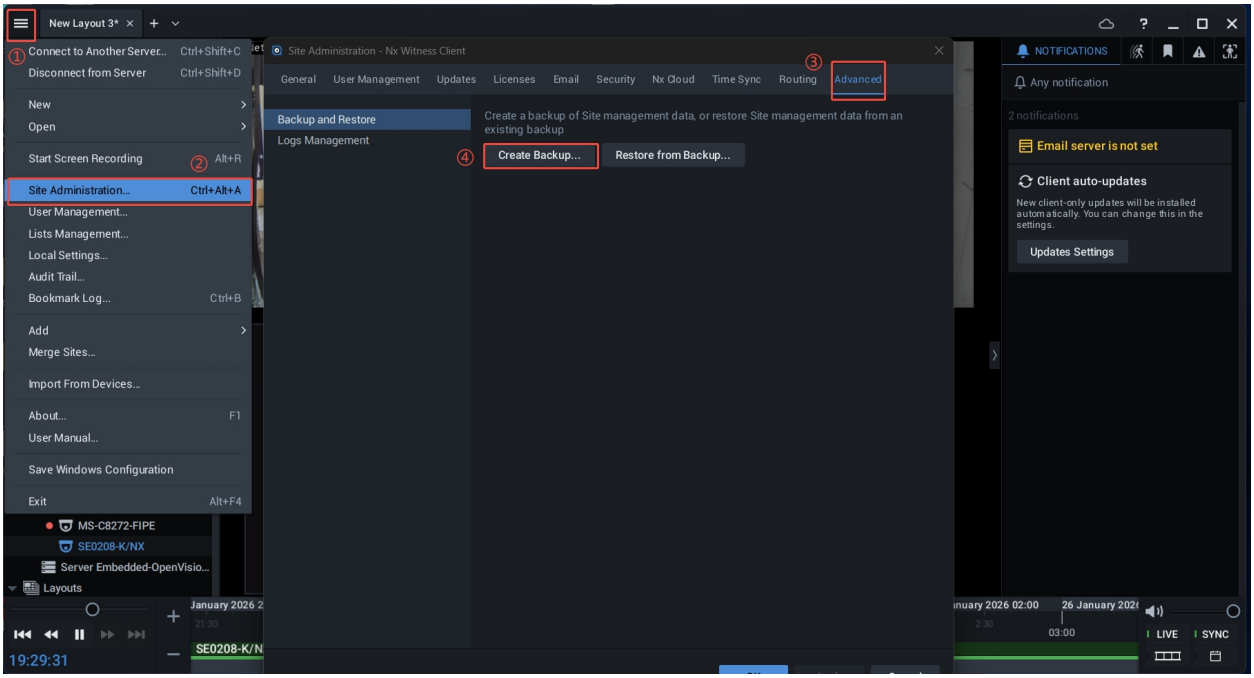
Method 2: Remote Reset

Remote reset can be performed via the Nx Witness Client. Users only need to click the designated reset button in the client to complete the operation.



Note:

It is strongly recommended to export your configuration before performing a hard reset. After the reset, you can import the configuration back into the system.

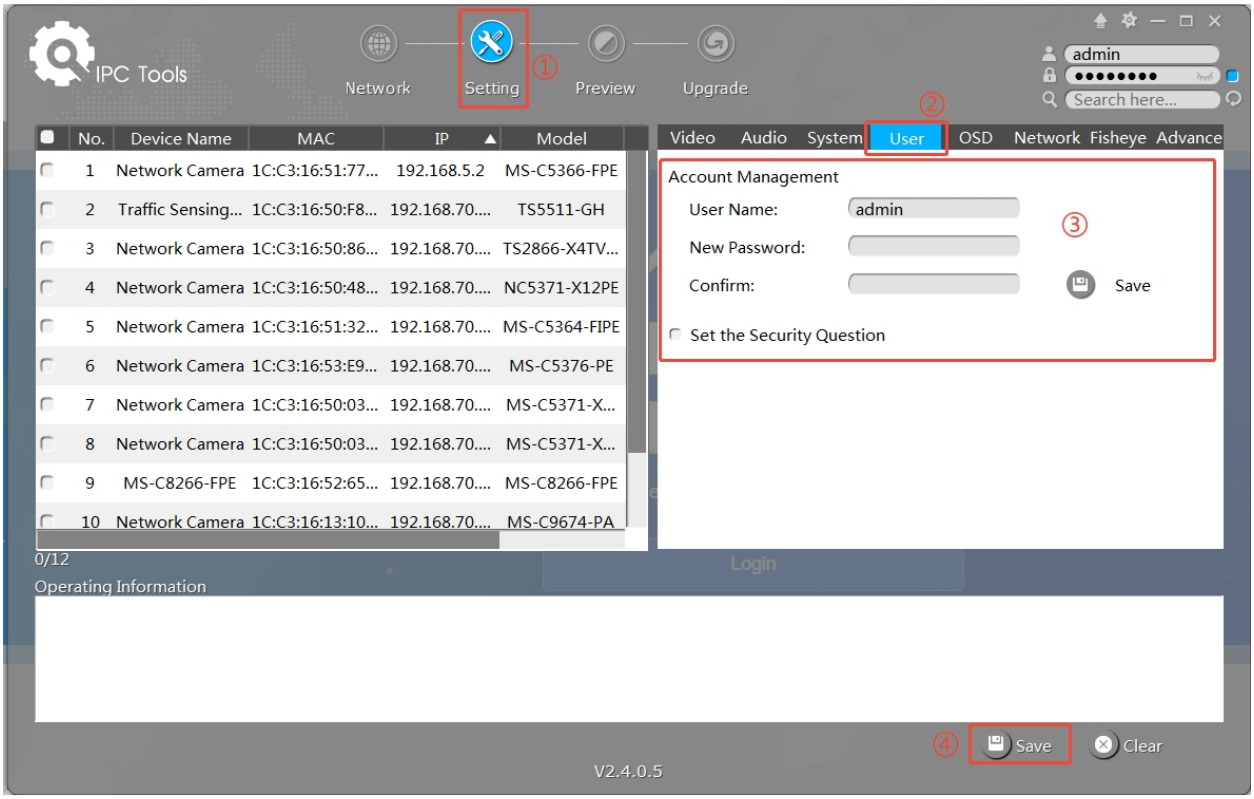


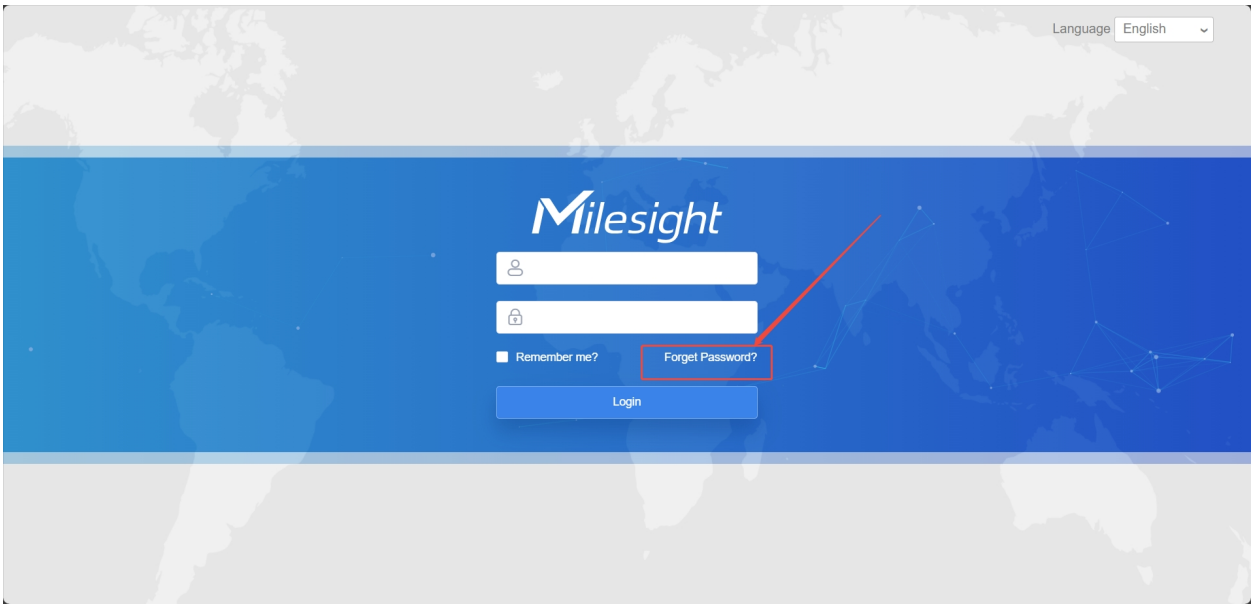
7.2.5 Password Reset

1. Reset Ubuntu Lock Screen Password

Method 1: Reset via Smart Tool or Web Interface

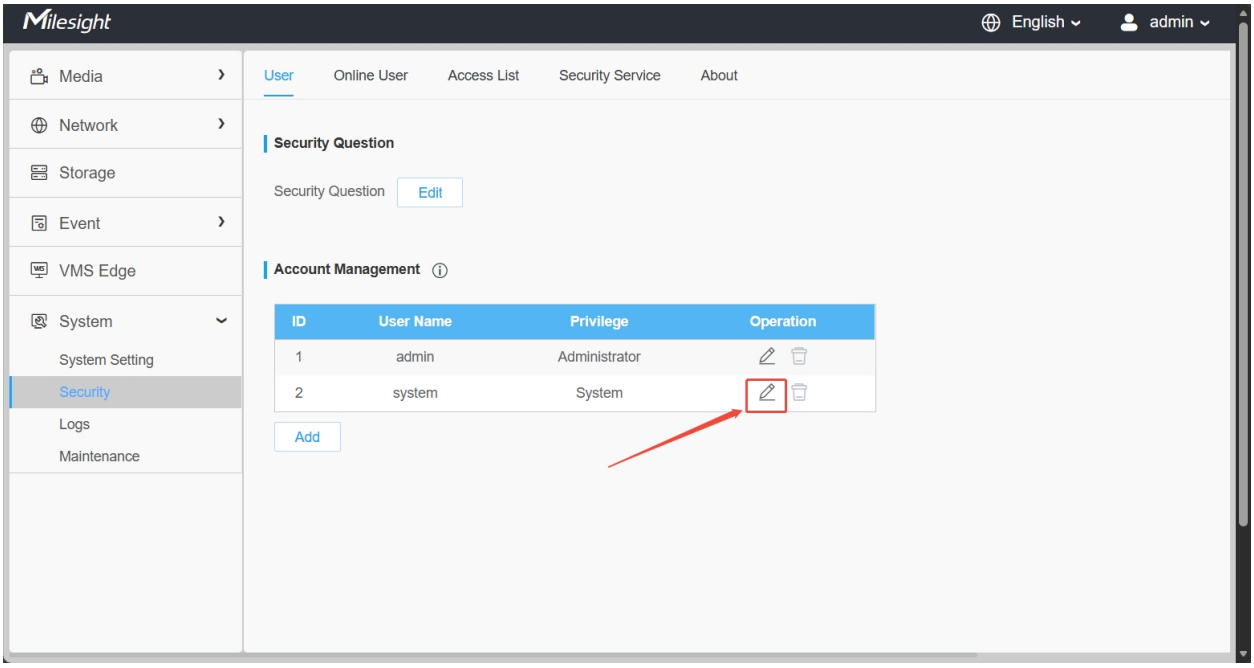
Use the Smart Tool or the web interface to reset the password (select "Forget Password"). The Ubuntu desktop password will also be reset to the factory default: **admin**.





Method 2: **Change Password via Web Interface**

You can modify the Ubuntu desktop password by updating the "system" account password through the web interface.



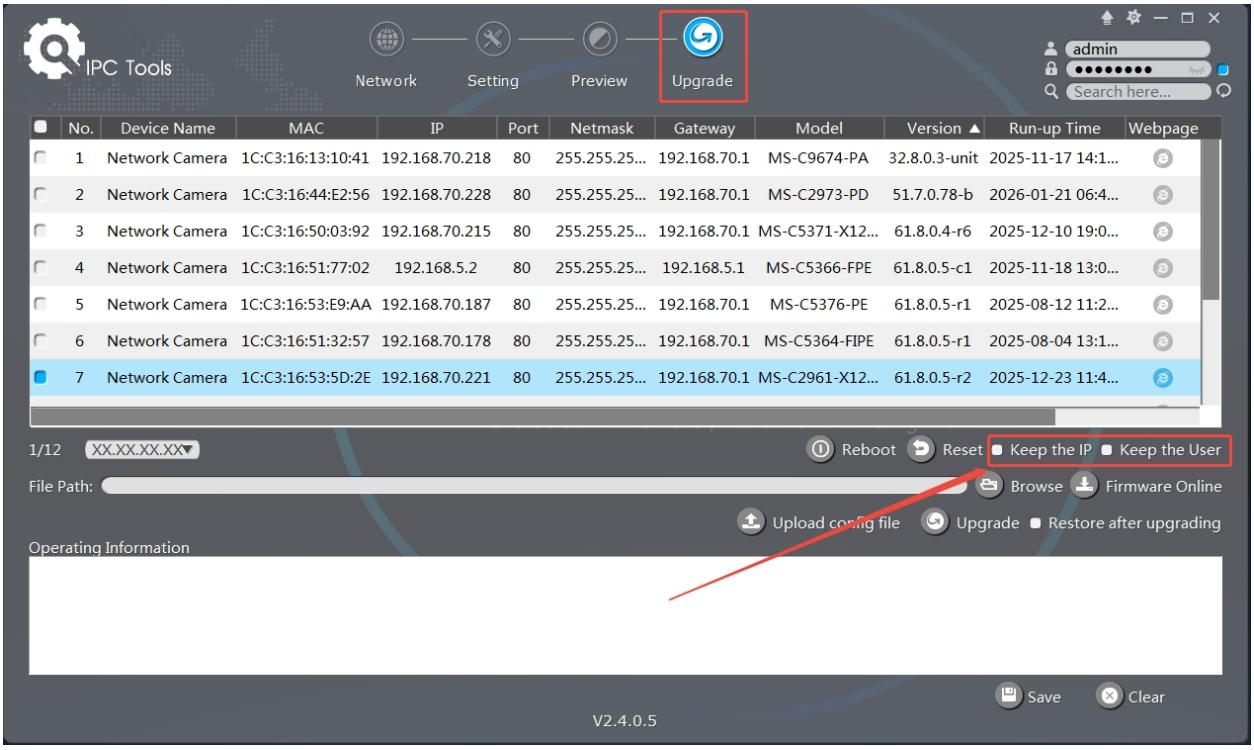
Method 3: Hardware Reset

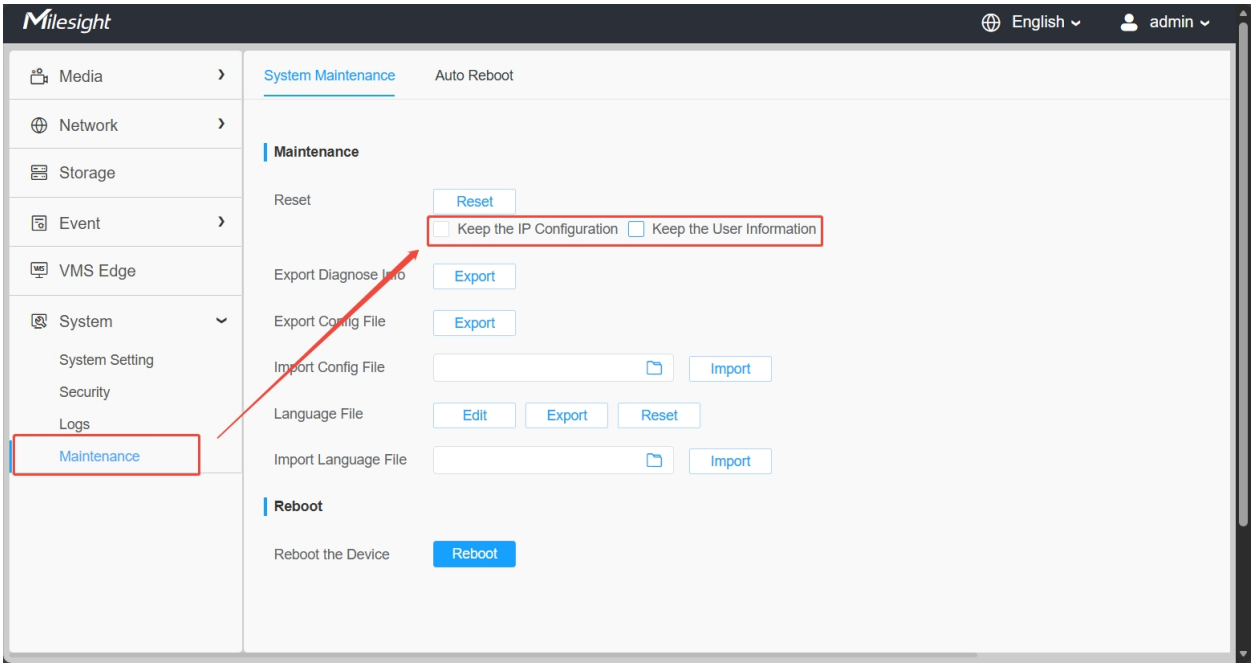
For detailed steps, please refer to Hard Factory Reset *(page 68)*. The Ubuntu desktop password will be reset to the factory default: **admin**.

2. Reset Nx Server Password

Method 1: Reset via Smart Tool or Web Interface

Use the Smart Tool or the web interface to reset the password (Uncheck "**Keep the IP**" and "**Keep the User**", and then click "**Reset**".). The Nx Server configuration will be reset to the initial state (system not created).





Method 2: Hardware Reset

For detailed steps, please refer to Hard Factory Reset *(page 68)*. The Nx Server configuration will be reset to the initial state (system not created).

Chapter 8. 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