Perimeter Protection Solution

User's Guide

V1.0.0

DAHUA TECHNOLOGY CO., LTD

Foreword

Safety Instructions

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

Signal Words	Meaning
WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

No.	Version	Revision Content	Release Time
1	V1.0.0	First Release.	January 2019

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Guide

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

- Upgrade the reader software or try other mainstream reader software if the Guide (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Guide are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

Electrical Safety

- All installation and operation should conform to your local electrical safety codes.
- The power source shall conform to the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited power Source requirement according to IEC60950-1. Please note that the power supply requirement is subject to the device label.
- Make sure the power supply is correct before operating the device.
- A readily accessible disconnect device shall be incorporated in the building installation wiring.
- Prevent the power cable from being trampled or pressed, especially the plug, power socket and the junction extruded from the device.

Environment

- Do not aim the device at strong light to focus, such as lamp light and sun light; otherwise it might cause over brightness or light marks, which are not the device malfunction, and affect the longevity of Complementary Metal-Oxide Semiconductor (CMOS).
- Do not place the device in a damp or dusty environment, extremely hot or cold temperatures, or the locations with strong electromagnetic radiation or unstable lighting.
- Keep the device away from any liquid to avoid damage to the internal components.
- Keep the indoor device away from rain or damp to avoid fire or lightning.
- Keep sound ventilation to avoid heat accumulation.
- Transport, use and store the device within the range of allowed humidity and temperature.
- Heavy stress, violent vibration or water splash are not allowed during transportation, storage and installation.
- Pack the device with standard factory packaging or the equivalent material when transporting the device.
- Install the device in the location where only the professional staff with relevant knowledge of safety guards and warnings can access. The accidental injury might happen to the non-professionals who enter the installation area when the device is operating normally.

Operation and Daily Maintenance

- Do not touch the heat dissipation component of the device to avoid scald.
- Carefully follow the instructions in the Guide when performing any disassembly operation about the device; otherwise, it might cause water leakage or poor image quality due to unprofessional disassemble. Please contact after-sale service for desiccant replacement if there is condensed fog found on the lens after unpacking or when the desiccant turns green. (Not all models are included with the desiccant).

- It is recommended to use the device together with lightning arrester to improve lightning protection effect.
- It is recommended to ground the device to enhance reliability.
- Do not touch the image sensor directly (CMOS). Dust and dirt could be removed with air blower, or you can wipe the lens gently with soft cloth that moistened with alcohol.
- Device body can be cleaned with soft dry cloth, which can also be used to remove stubborn stains when moistened with mild detergent. To avoid possible damage on device body coating which could cause performance decrease, do not use volatile solvent such as alcohol, benzene, diluent and so on to clean the device body, nor can strong, abrasive detergent be used.
- Dome cover is an optical component, do not touch or wipe the cover with your hands directly during installation or operation. For removing dust, grease or fingerprints, wipe gently with moisten oil-free cotton with diethyl or moisten soft cloth. You can also air blower to remove dust.

- Please strengthen the protection of network, device data and personal information by adopting measures which include but not limited to using strong password, modifying password regularly, upgrading firmware to the latest version, and isolating computer network. For some device with old firmware versions, the ONVIF password will not be modified automatically along with the modification of the system password, and you need to upgrade the firmware or manually update the ONVIF password.
- Use standard components or accessories provided by manufacturer and make sure the device is installed and maintained by professional engineers.
- The surface of the image sensor should not be exposed to laser beam radiation in an environment where a laser beam device is used.
- Do not provide two or more power supply sources for the device unless otherwise specified. A failure to follow this instruction might cause damage to the device.

Cybersecurity Recommendations

Mandatory cybersecurity actions

1. Change Passwords and Use Strong Passwords:

The number one reason systems get “hacked” is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

Recommendations to improve your network security

1. Change Passwords Regularly

Regularly change the credentials to your devices to help ensure that only authorized users are able to access the system.

2. Change Default HTTP and TCP Ports:

● Change default HTTP and TCP ports for systems. These are the two ports used to communicate and to view video feeds remotely.

● These ports can be changed to any set of numbers between 1025-65535. Avoiding the default ports reduces the risk of outsiders being able to guess which ports you are using.

3. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

4. Enable IP Filter:

Enabling your IP filter will prevent everyone, except those with specified IP addresses, from accessing the system.

5. Change ONVIF Password:

On older IP Camera firmware, the ONVIF password does not change when you change the system’s credentials. You will need to either update the camera’s firmware to the latest revision or manually change the ONVIF password.

6. Forward Only Ports You Need:

● Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.
● You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

7. Disable Auto-Login on SmartPSS:

Those using SmartPSS to view their system and on a computer that is used by multiple people should disable auto-login. This adds a layer of security to prevent users without the appropriate credentials from accessing the system.

8. Use a Different Username and Password for SmartPSS:

In the event that your social media, bank, email, etc. account is compromised, you would not want someone collecting those passwords and trying them out on your video surveillance system. Using a different username and password for your security system will make it more difficult for someone to guess their way into your system.

9. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

10. UPnP:

● UPnP will automatically try to forward ports in your router or modem. Normally this would be a good thing. However, if your system automatically forwards the ports and you leave the credentials defaulted, you may end up with unwanted visitors.
● If you manually forwarded the HTTP and TCP ports in your router/modem, this feature should be turned off regardless. Disabling UPnP is recommended when the function is not used in real applications.

11. SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

12. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

13. Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

14. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

15. Connect IP Cameras to the PoE Ports on the Back of an NVR:

Cameras connected to the PoE ports on the back of an NVR are isolated from the outside world and cannot be accessed directly.

16. Isolate NVR and IP Camera Network

The network your NVR and IP camera resides on should not be the same network as your public computer network. This will prevent any visitors or unwanted guests from getting access to the same network the security system needs in order to function properly.

Table of Contents

1 Overview

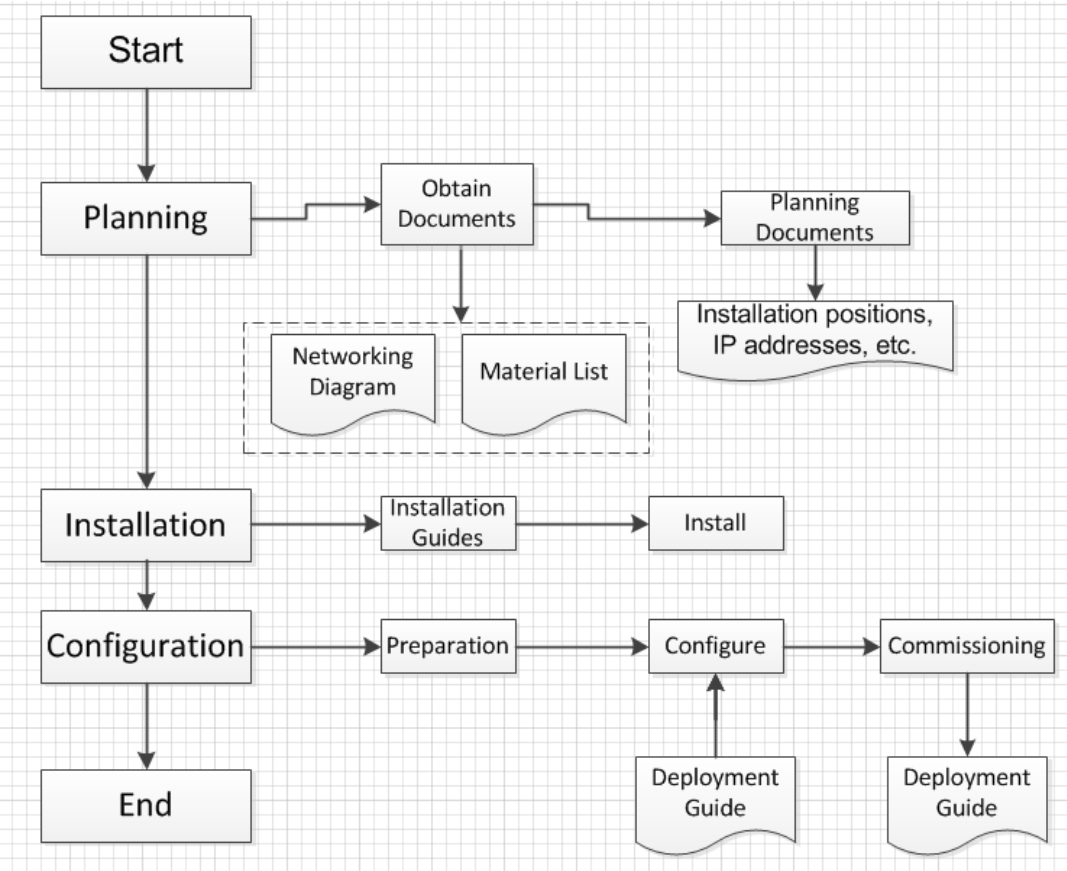
Perimeter protection is the most fundamental system in public security, and also the most important defense against illegal invasion and other events. This solution covers user's demands of monitoring perimeter areas and key areas and provides detections against area invasion, tripwire and other events. It can also classify and detect humans and vehicles with high accuracy and perform further filter to reduce false alarm, with video surveillance and behavior analysis, users can realize visual management easily.

The key feature of this solution is AI algorithm, which classifies humans and vehicles and performs further filter to reduce false alarm. This solution achieved better accuracy than the previous ones with frequent false alarms caused by IR interference and electric fence, it is applicable to cover the monitoring needs for industrial parks, schools, factories, and warehouses.

2 Deployment Process

This process includes planning, installation, and configuration, and you might need to refer to all the provided documents and produce your own planning document. See Figure 2-1.

Figure 2-1 Deployment process



3 Planning

3.1 Required Documents

Material list and networking diagram are needed during planning and deployment.

3.1.1 Material List

You need to obtain this list from project leader. See Table 3-1.

During deployment, if the actual software version is older than the listed ones, you need to update them to the latest version, and if the actual software version is newer than the listed ones, then they are ready for use.

Table 3-1 Material List

Device	Model	Software version	Material number
DSS Express	-	2.7.01.02.00224 General_DSS-Express_IS_V1.000.0000002.0.R.20181114.exe	-
DMSS	-	• For iOS: idmss plus 4.20.001 • For Android: gdmss plus 4.20.000	-
NVR	NVR5208-8P-4KS2(V2.0)	2.6.01.02.01859 DH_NVR5XXX-4KS2_MultiLang_V3.216.0000004.0.R.20181229.zip	1.0.01.23.11906 (EU) 1.0.01.23.12056 (UK) 1.0.01.23.12034 (US)
	NVR5216-16P-4KS2E	2.6.01.02.01859 DH_NVR5XXX-4KS2_MultiLang_V3.216.0000004.0.R.20181229.zip	1.0.01.23.11991 (EU) 1.0.01.23.12074 (UK) 1.0.01.23.12052 (US)
	NVR5416-16P-4KS2E	2.6.01.02.01859 DH_NVR5XXX-4KS2_MultiLang_V3.216.0000004.0.R.20181229.zip	1.0.01.23.11910 (EU) 1.0.01.23.12067 (UK) 1.0.01.23.12045 (US)
	NVR5208-4KS2(V2.0)	2.6.01.02.01859 DH_NVR5XXX-4KS2_MultiLang_V3.216.0000004.0.R.20181229.zip	1.0.01.23.11905 (EU) 1.0.01.23.12053 (UK)

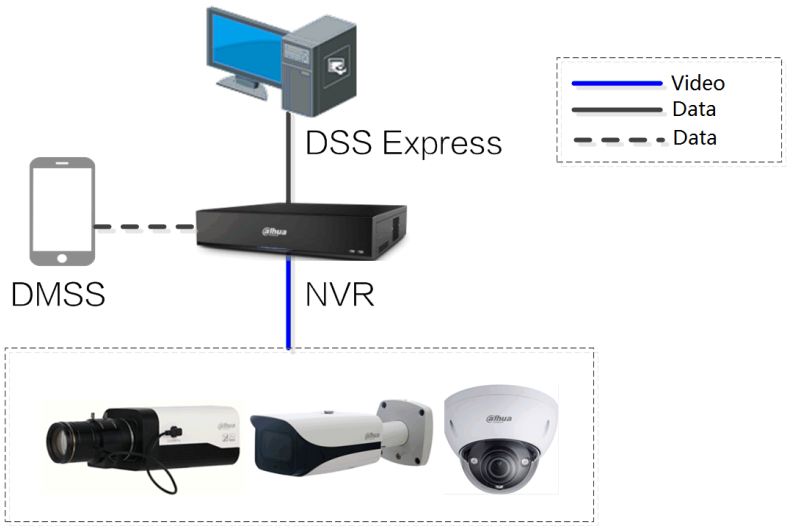
Device	Model	Software version	Material number
			1.0.01.23.12031 (US)
	NVR5216-4KS2(V2.0)	2.6.01.02.01859 DH_NVR5XXX-4KS2_MultiLang_V3.216.0000004.0.R.20181229.zip	1.0.01.23.11907 (EU) 1.0.01.23.12054 (UK) 1.0.01.23.12032 (US)
	NVR5416-4KS2(V2.0)	2.6.01.02.01859 DH_NVR5XXX-4KS2_MultiLang_V3.216.0000004.0.R.20181229.zip	1.0.01.23.11909 (EU) 1.0.01.23.12059 (UK) 1.0.01.23.12037(US)
	NVR4108HS-8P-4KS2	2.6.01.02.01850 DH_NVR4XXX-4KS2_MultiLang_V3.216.0000002.0.R.190102.zip	1.0.01.23.11290 (EU) 1.0.01.23.11568 (UK) 1.0.01.23.11597(US)
	NVR4216-16P-4KS2	2.6.01.02.01850 DH_NVR4XXX-4KS2_MultiLang_V3.216.0000002.0.R.190102.zip	1.0.01.23.11193 (EU) 1.0.01.23.11575 (UK) 1.0.01.23.11604(US)
Camera	DH-IPC-HFW8241EP-Z-27135	2.6.01.05.04953：DH_IPC-HX8X4X-Warpway2_EngSpnFrn_PN_Stream3_V2.622.0000000.9.R.181119.zip	1.0.01.04.27497
	DH-IPC-HFW8241EN-Z-27135	2.6.01.05.04950：DH_IPC-HX8X4X-Warpway2_EngSpnFrn_NP_Stream3_V2.622.0000000.9.R.181119.zip	1.0.01.04.28342
	DH-IPC-HFW8241EP-Z-0735	2.6.01.05.04953：DH_IPC-HX8X4X-Warpway2_EngSpnFrn_PN_Stream3_V2.622.0000000.9.R.181119.zip	1.0.01.04.27499
	DH-IPC-HFW8241EN-Z-0735	2.6.01.05.04950：DH_IPC-HX8X4X-Warpway2_EngSpnFrn_NP_Stream3_V2.622.0000000.9.R.181119.zip	1.0.01.04.28344
	DH-IPC-HFW3241EP-Z-27135	2.6.01.05.04615：DH_IPC-HX3XXX-Sag_EngSpnFrn_PN_Stream3_V2.622.0000000.15.R.181102.zip	1.0.01.04.27567

Device	Model	Software version	Material number
	DH-IPC-HFW3241 EN-Z-27135	2.6.01.05.04612：DH_IPC-HX3XXX-Sag_EngSpnFrn_NP_Stream3_V2.622.0000000.15.R.181102.zip	1.0.01.04.27568
	DH-IPC-HFW3241 EP-Z-0735	2.6.01.05.04615：DH_IPC-HX3XXX-Sag_EngSpnFrn_PN_Stream3_V2.622.0000000.15.R.181102.zip	1.0.01.04.27571
	DH-IPC-HFW3241 EN-Z-0735	2.6.01.05.04612：DH_IPC-HX3XXX-Sag_EngSpnFrn_NP_Stream3_V2.622.0000000.15.R.181102.zip	1.0.01.04.27572

3.1.2 Networking Diagram

This diagram shows how all devices connect to each other in this solution. See Figure 3-1.

Figure 3-1 Networking diagram



3.2 Collecting and Planning Data

After all the preparations are done, you can open the attached table and plan the device information, installation position, and IP addresses. You can modify the content in the table as needed.

Planning Table.xlsx

4 Installation

You need to confirm whether all the devices work properly, and then you can start deployment and configuration.

4.1 Installation Guides

The following devices are included in this solution, and you can see the installation method in each installation guide. See Table 4-1.

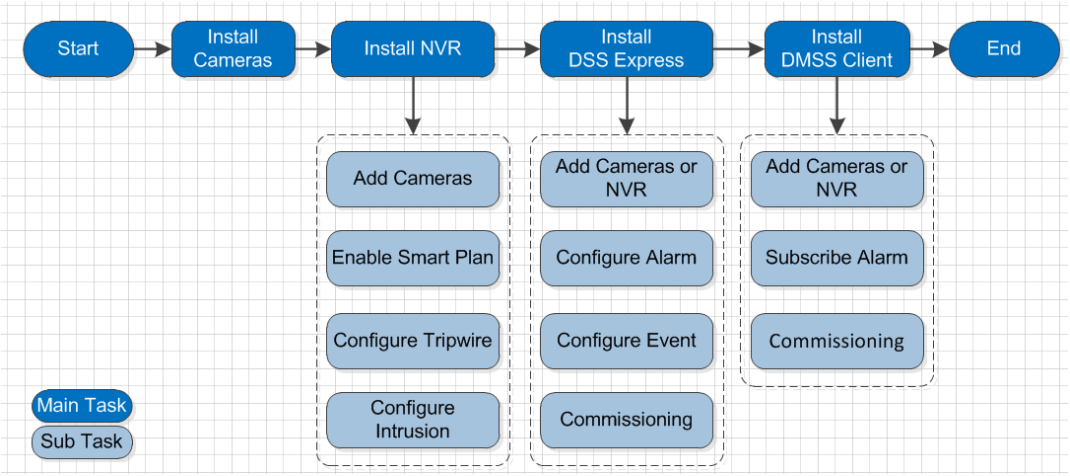
Table 4-1 Installation guides

No.	Device	Installation guide name	Guide location
1	Camera	Network Camera_Quick Start Guide	Document kit
2	NVR	NVR_User's Manual	Document kit
3	DSS Express	DSS Express_User's Manual	Document kit or the provided manual
4	DMSS	DMSS Mobile app_User's Manual	Document kit or the provided manual

4.2 Installation Process

With proper installation guide, you can install all the devices with the following process. See Figure 4-1 .

Figure 4-1 Installation process



4.3 Installing Cameras

Installation site and installation type are essential to the final performance, this section introduces how to select proper installation site and installation type, and how to configure image parameters.

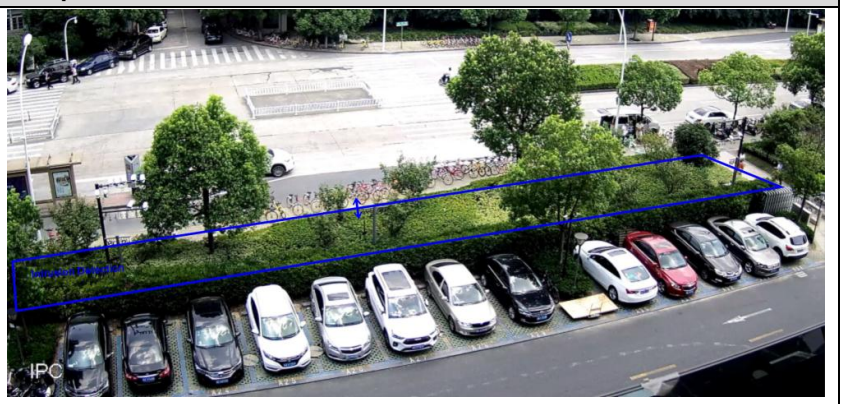
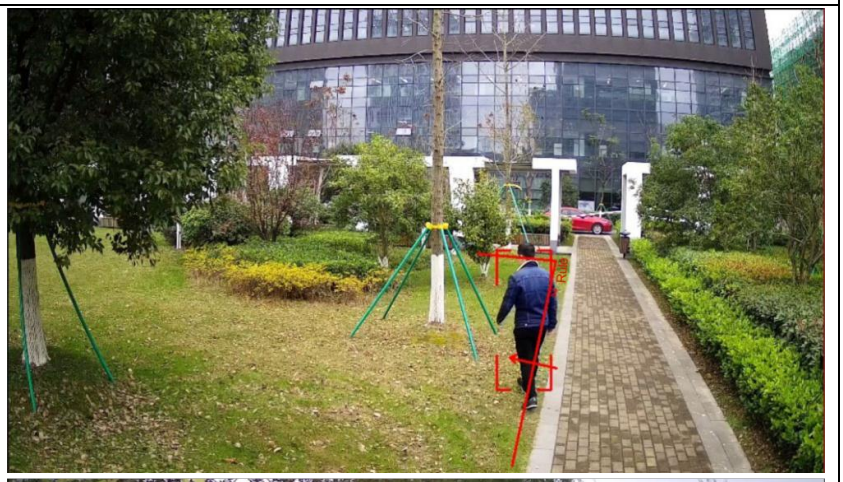
See the corresponding quick start guide for the installation details.

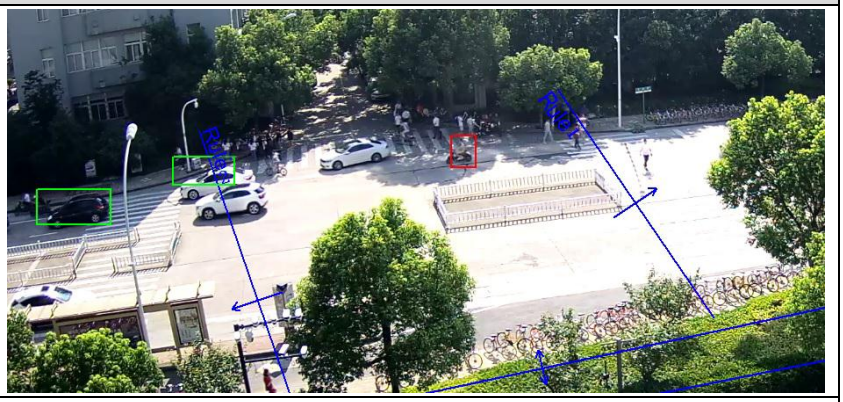
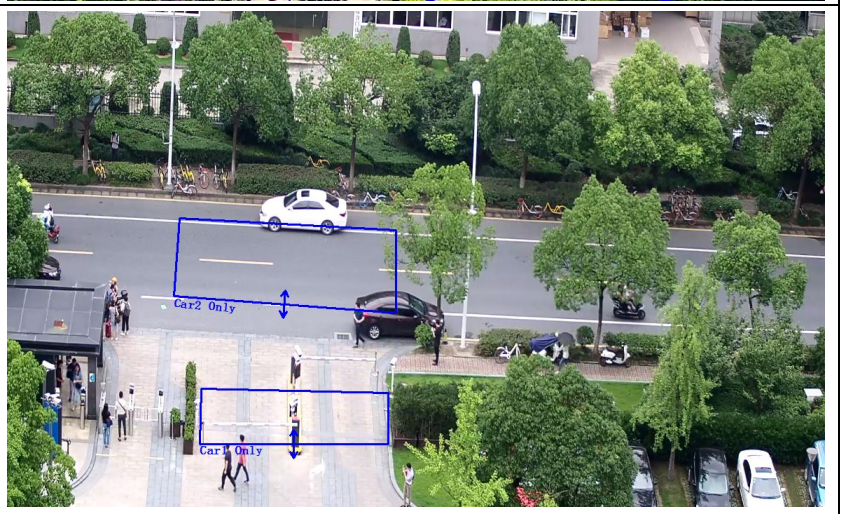
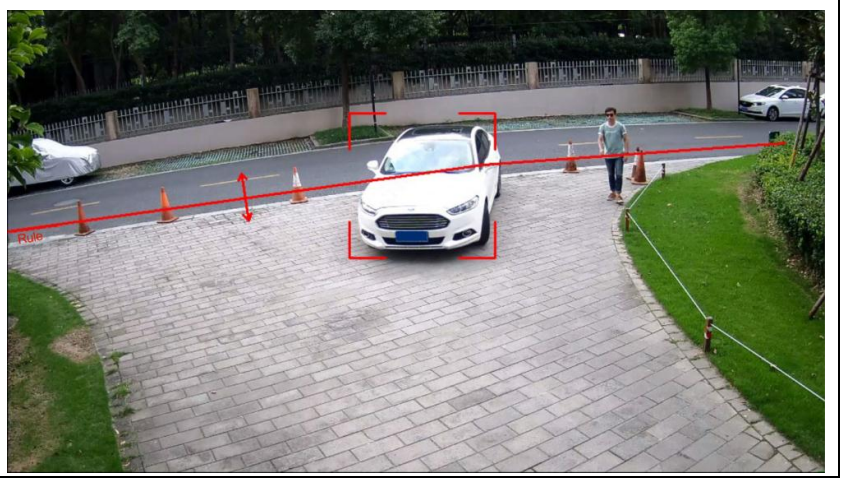
4.3.1 Installation Site

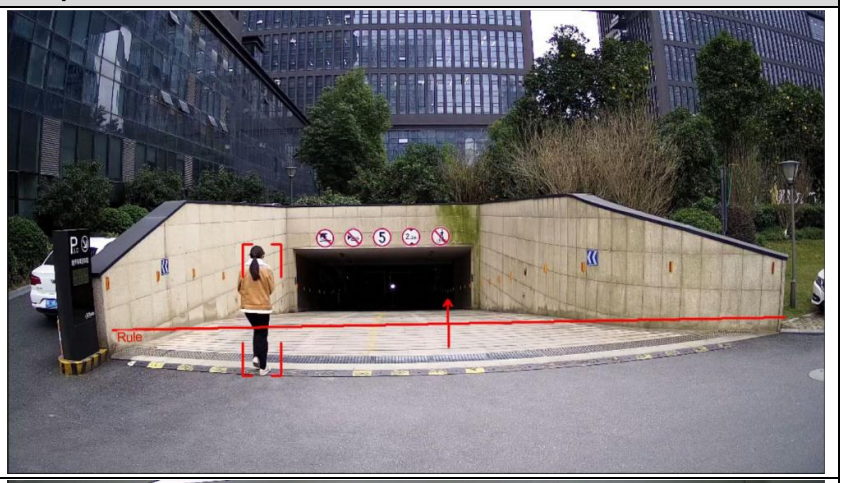
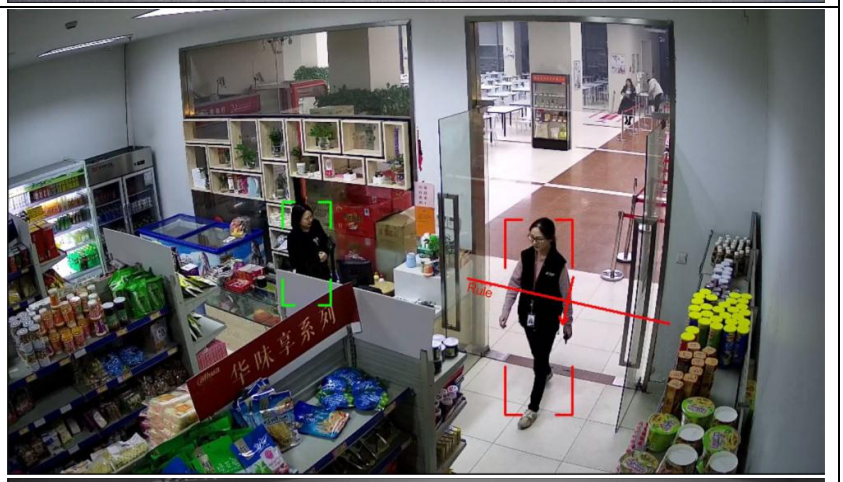
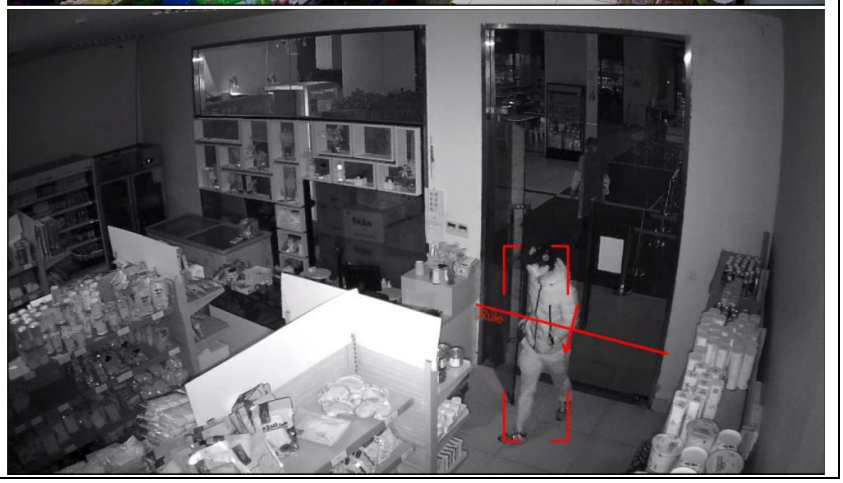
This section introduces suitable sites and unsuitable sites, you need try to select suitable ones and avoid unsuitable ones.

Suitable Sites

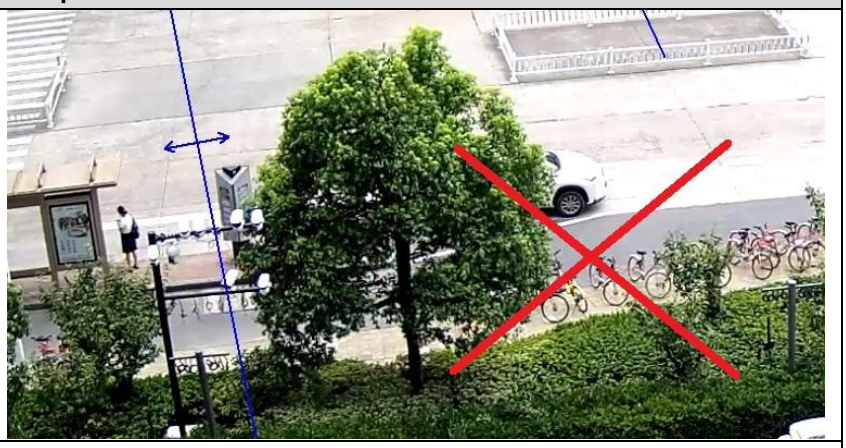
The sites need to provide grand visual field and be open and simple, and there are no frequent moving objects or drastic change in lighting condition. This kind of sites are suitable for cross detection at borderlines, communities, lawns, railways, and highways, access detection at underground garages, pedestrian streets, fall detection at lakes, and access detection at rooftops and private properties. See the following table for examples.

Examples	Site picture
Configure intrusion rule along obvious perimeters, such as green plant.	 
Configure intrusion rule along obvious perimeters, such as lawns and lakes.	 

Examples	Site picture
Install cameras at high position perpendicular to the road to monitor humans and vehicles.	
Install cameras at park or garage entrances to detect human who goes into motorway or vehicles which goes into pedestrian area.	 

Examples	Site picture
	
Configure tripwire rule at store entrances.	 

Unsuitable Sites

Examples	Site picture
Large obstacles around the target area that blocked target objects.	
Vehicle headlights on the road makes drastic changes of lighting condition, which influences detection performance.	
The ambient light is too dark, and cameras have poor performance under black and white mode.	

4.3.2 Installation Requirements

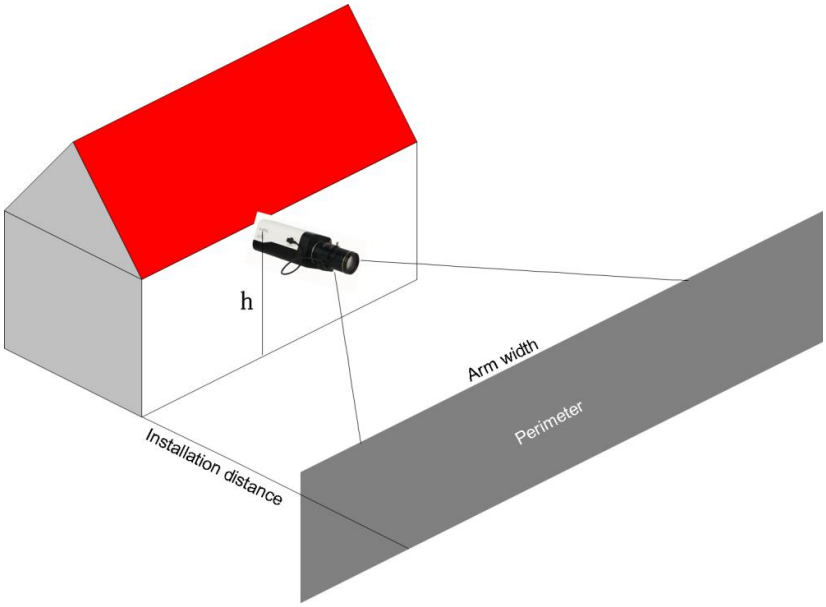
This section introduces the pixel size requirement for target recognition with different installation types.

Installing Cameras toward the Perimeter

You can install cameras on the nearby buildings or poles toward the perimeter.

When the resolution is 1080p, the minimum pixel size requirements are: 60×60 for 8241 series; 70×70 for 3241 series.

Figure 4-2 Installation Diagram (1)



Install cameras with the following instructions, and the shorter the installation distance is, the smaller the arm width will be.

- The maximum arm width against human for 8241 series is 12m.
  Refer to the following table for the matching relationship between different lenses and installation distances for 8241 series.

Lens's focal length (mm)	2.8	3.6	6.0	8.0	12	30
Installing distance (m)	6	8	13	17	26	65

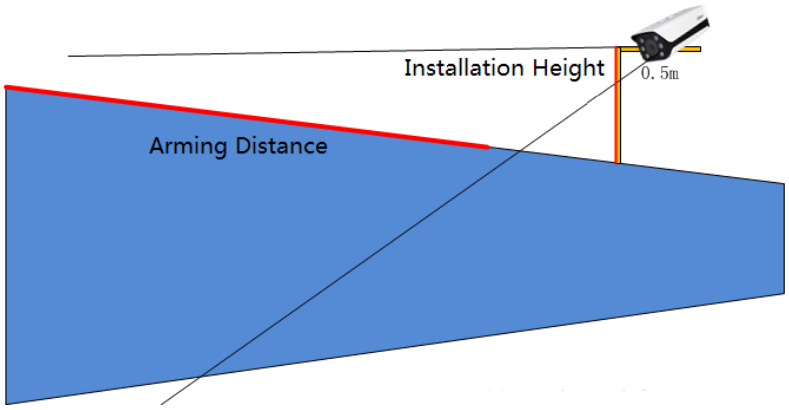
- The maximum arm width against human for 3241 series is 12m.
  - ◇ When the installing distance is 5m~22 m, it is recommended to select the lens which focal length is 2.7mm~13.5 mm.
  - ◇ When the installing distance is 13m~55m, it is recommended to select the lens which focal length is 7mm~35mm.
- Recommended installing height: h > 3m, and the maximum height varies with different lens.
- Recommended installing angle: 0°～45° (elevation angle).
- Recommended lens: Low focal length, and large angle of view.

Installing Cameras along the Perimeter

You can install cameras on the perimeter with its direction along the perimeter.

When the resolution is 1080p, the minimum pixel size requirements are: 60×60 for 8241 series; 70×70 for 3241 series.

Figure 4-3 Installation Diagram (2)



When installing cameras on the perimeter, there might be blind area, and you can install two cameras face to face to realize monitoring without blind area.

- Refer to the following table for the matching relationship between different lenses and installation distances for 8241 series.

Lens's focal length (mm)	**2.8**	**12**	**8**	**30**
Arming distance (m)	1～6	4～25	3～17	12～60

- Refer to the following table for the matching relationship between different lenses and installation distances for 3241 series.

Lens's focal length (mm)	**2.8**	**12**	**8**	**30**
Arming distance (m)	1～5	4～22	3～14	12～50

When there are people trying to climb over the perimeter, the shape of its model changes, so it is recommended to select lens with 0735 focal length, and the installation height is 1 m above the perimeter. Then the arming distance can reach 12m–60m. You can install two cameras face to face to realize monitoring without blind area.

4.3.3 Configuring Images

After installing cameras, you can login the web interface and configure the image as needed. See more details in the web operation manual.

Normally you can keep the default parameters, and you need to ensure that the target edge is clear at night.

When the image is over exposed or too dark, you might need to enable WDR.

The followings are scenarios that require WDR and the comparisons before and after WDR.

- Scenarios 1: Back light is too strong

After enabling WDR:

- Scene 2: Over exposed

After enabling WDR:

5 Configuration

5.1 Configuration Process

After installation, you need to configure and connect all the devices to make the whole solution work. See Table 5-1.

Table 5-1 Configuration process

Device	Description	Target section
Camera	Initialize cameras and modify IP addresses.	5.3Configuring Cameras
NVR	1. Adding Cameras 2. Enabling Smart Plan 3. Configuring IVS Rules	5.4Configuring NVR
DSS Express	1. Add device 2. Configuring Alarm 3. Configuring Alarm Events	5.5Configuring DSS Express
DMSS client	1. Add device 2. Subscribing Alarm	5.6Configuring DMSS Client

5.2 Preparation

One laptop with Windows system; install the ConfigTool from Dahua tool kit; install IE8 explorer.

5.3 Configuring Cameras

- For brand new cameras, see the quick start guide and web operation manual to initialize cameras and modify IP addresses.
- For cameras that are properly configured, be sure to update the system to the latest version.

5.4 Configuring NVR

5.4.1 Preparation

- For brand new NVR, see the quick start guide and web operation manual to initialize them and modify IP addresses.
- For NVR that are properly configured, be sure to update the system to the latest version.

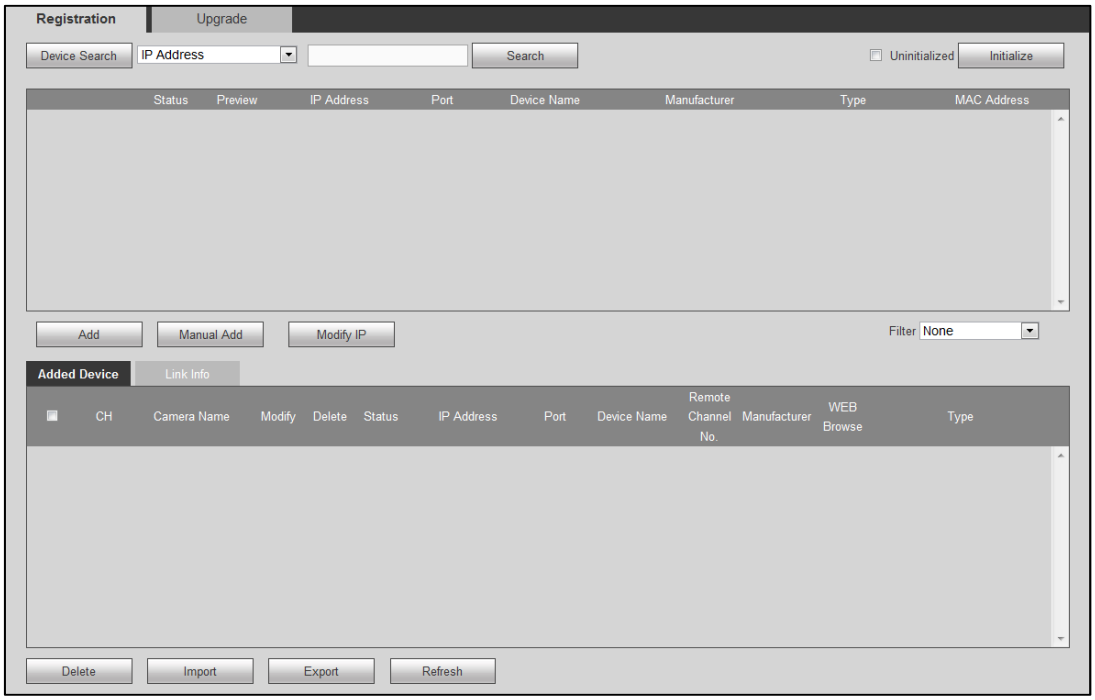
5.4.2 Adding Cameras

You can add cameras to the NVR and manage them remotely.

Step 1 Log in the NVR web interface, and then select **SETUP > IMAGE > REGISTRATION**.

The **REGISTRATION** interface is displayed. See Figure 5-1.

Figure 5-1 REGISTRATION (1)



Step 2 Add devices

You can add cameras with auto scan, manual search or template.

The target camera can not have the same IP address or TCP port with any existing camera.

- Auto scan
  1. Click **Device Search**.
     The system will start scanning all the available devices, after the searching progress goes to 100%, all the devices are displayed, including cameras, NVR, and other devices, and you can select **IPC** from the **Filter**. See Figure 5-2. And for the detailed introduction, see Table 5-2.
  2. Double click the device information or select the check box in front of it, and then click **Add**, the device will be added to the **Added Device** list.

You can refresh the **Added Device** list to avoid adding the same camera repeatedly.

Figure 5-2 REGISTRATION (2)

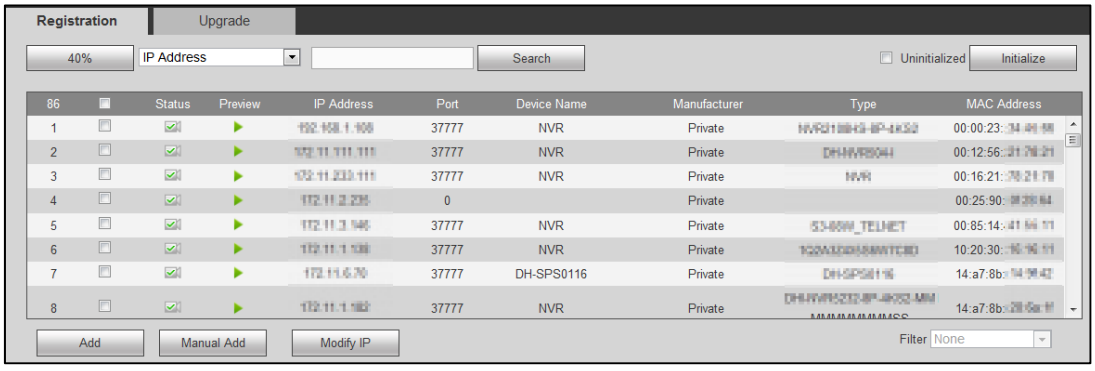
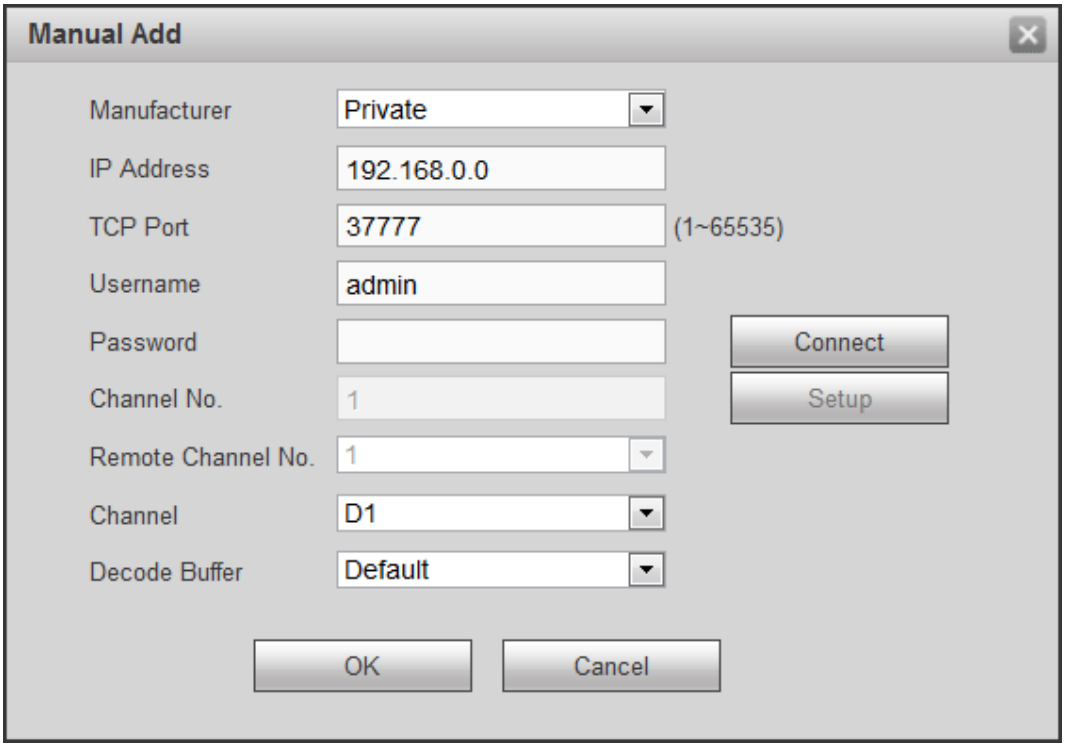


Table 5-2 Parameter description

Icon/Parameter	Description
IP Address	Select **IP Address** or **MAC Address** from the list, then input the IP address or MAC address of the device you need, and then click **Search** to find it.
Uninitialized	Select the **Uninitialized** check box, and then all the devices that have not been initialized are listed. Select the devices you need, and then click **Initialize** to configure user name and password for them. See more details in their user's manuals.
Status	Shows whether a device is initialized. means it is initialized; means it is uninitialized**.**
IP Address	Shows the IP address, port number, name, manufacturer, type, and MAC address of a device.
Port	
Device Name	
Manufacturer	
Type	
MAC Address	
Modify IP	Select one or multiple the devices, and then click **Modify IP** to change their IP addresses. See more details in their user's manuals.
Filter	Select the device type or model you need to display them.

- Manual search
  1. Click **Manual Add**.
     The **Manual Add** interface is displayed. See Figure 5-3.

Figure 5-3 Manual add



  2. Configure parameters. See Table 5-3.

Table 5-3 Manual add parameters

Parameter	Description
Manufacturer	Select **Private**. Supported protocol might vary with different models, and the actual product shall prevail.
IP Address	Input the IP address of the target camera.
RTSP Port	Input the RTSP port of the target device, and it is 554 by default. This is not needed when the **Manufacturer** is configured to **Private** or **Customized**.
HTTP Port	Input the HTTP port of the target device, and it is 80 by default. This is not needed when the **Manufacturer** is configured to **Private** or **Customized**.
TCP Port	Transmission control protocol port, the value is 37777 by default.
Username/Password	Input the user name/password of the camera you need.
Channel No.	Click **Connect**, and then the video stream quantity of the target camera is displayed at Channel No., and this is not editable. The system will add all video streams to the NVR. ● It is recommended to click **Connect** to obtain the number. If the channel number is wrong, the operation will fail. ● If the target device is human body recognition camera, you must click **Connect** to obtain the number.
Remote channel No.	If the target camera has already connected to another NVR, then its channel No. on that NVR is displayed here.
Channel	Displays the channel No. on your NVR to which you connect the target camera to.
Decode Buffer	You can select from **Default**, **Real time**, and **Fluent**. **Real time**provides best live video quality, but also requires network with fast speed to respond to IVS detection, **Default** is medium, and **Fluent** is the safest choice.

3. Click **OK**.

- Import from Template
  1. You can export the template from other NVR, and then import to your NVR.
     - ◇ Templates with different languages as your NVR are not compatible.
     - ◇ You cannot open and view encrypted templates.
  2. Click **Import** to select the template you need.
     If there are cameras in the template which IP addresses are already existed, there will be a notice, and you can select whether to overwrite or to add new IP address.

Step 3 You can view the camera connection status at **Added Device**.
For the detailed description, see Table 5-4.

Table 5-4 Added device interface description

Parameter	Description
CH	The channel No. on your NVR to which you connected the video stream to.
Modify	Click to modify device information. See Table 5-3.
Delete	Select one or multiple devices, and then click to delete them from your NVR.
Status	Shows the device connection status. Means online; means offline.
IP Address	Shows the IP address, port number, name, manufacturer, type, and MAC address of a device.
Port	
Device Name	
Remote Channel No.	
Manufacturer	
WEB Browse	If the icon shows , click it to visit the web interface of the device, and you can configure this device as needed.
Type	Shows the device type or model.

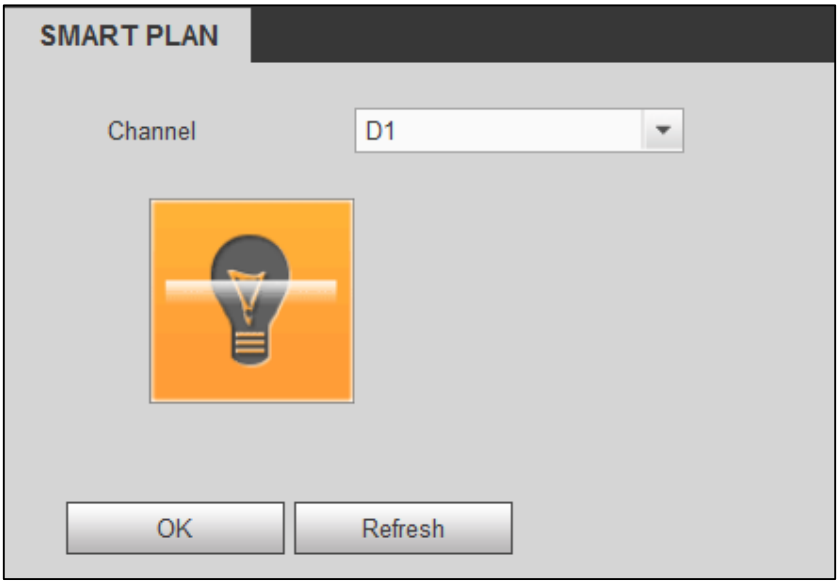
5.4.3 Enabling Smart Plan

You need to enable the smart plan first, and then configure all the rules under this plan.

Step 1 Log in the NVR web interface, and then select **SETUP > EVENT > SMART PLAN**.

The **SMART PLAN** interface is displayed, see Figure 5-4.

Figure 5-4 Smart plan



Step 2 Select the video stream in which you need to enable smart plan with its channel No., and then click the plan you need.

The plan will be highlighted after being enabled, click it again to disable it.

Step 3 Click **OK**.

5.4.4 Configuring IVS Rules

This section introduces how to configure tripwire and intrusion rules, and if the rules are triggered, there system will send alarm.

5.4.4.1 General Instructions

- The target pixel size need to meet certain conditions to be successfully recognized by the AI algorithm.
  - ◇ Video resolution should be 1080p or above.
  - ◇ When the resolution is 1080p, the minimum pixel size requirements are: 60×60 for 8241 series; 70×70 for 3241 series.
- The target height should be smaller than 2/3 of the image height; the brightness difference of the target and the background should be no less than 10 gray levels.
- Keep the tripwire ruler vertical to the target moving direction as much as possible, and avoid drawing curved lines since they might cause detection failure.
- Keep the rulers at the center of the image as much as possible, and make sure the target is visible for longer than 0.5 s before reaching the ruler. The target should be present in the image for no less than 2 consecutive seconds, and the moving distance should be larger than its width and no less than 15 pixels （CIF image） at the same time. If the target has already crossed the rulers even before they appear in the image completely, the detection will fail.
- Try to avoid scenes with obstacles such as trees, buildings that might block the target moving track; scenes with reflective surfaces such as glass, bright ground or water; scenes that disturbed by tree branches, shadows or winged insects; scenes that against light or under direct light exposure; scenes that have too many targets or with drastic changes of lighting condition; scenes that already have human or vehicles in them.

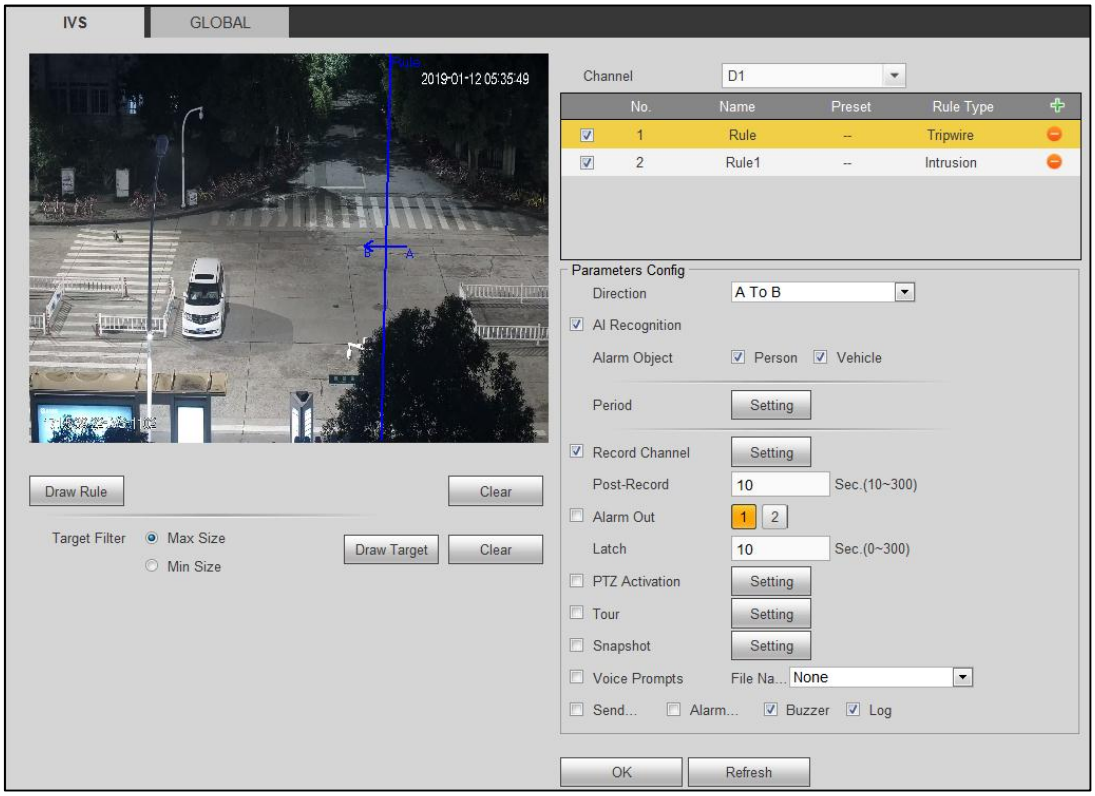
5.4.4.2 Tripwire

When any target crosses the ruler with the defined direction, the rule will be triggered.

Step 1 Select **SETUP > EVENT > IVS > IVS**.
The **IVS** interface is displayed.

Step 2 Select the video stream in which you need to configure IVS rule with its channel No., and then click to add a rule. Double click the words at **Name** column to input the rule name; double click the value at **Rule Type** column, and then select **Tripwire**. See Figure 5-5.

Figure 5-5 Tripwire



Step 3 Click **Draw Rule**, and then draw the ruler in the image, right click to finish drawing.

Step 4 It requires certain time and moving space for the target to be confirmed, so leave some space at both sides of the ruler during configuration and do not draw it near obstacles.

Click **Clear** to delete the existing rulers.

Step 5 Select **Max Size** or **Min Size** at **Target Filter**, and then click **Draw Target** to draw the box.

- Only the targets with the size between **Max Size** and **Min Size** are valid.
- Select **Max Size** or **Min Size** at **Target Filter**, and then click the **Clear** at the right side of **Draw Target** to delete the box.

Step 6 Configure tripwire parameters. See Table 5-1.

Table 5-1 Tripwire parameter description

Parameter	Description

Parameter	Description
Working period	Configure working period, and the rule takes effect only within this period. 1. Click **Setting** at **Period**, and then the period setting interface is displayed. 2. Configure each period. ● A: Press and hold the left mouse button, and then drag at the periods you need. ● B: Click the **Setting** behind the week day you need, and then the week day in the period setting box shows red color, select and configure the periods you need, and you can configure 6 periods in one week day at most. 3. Click OK.
Direction	Configure the tripwire direction, you can select **A->B**, **B->A** and **A<->B**.
AI Recognition	Select the **AI Recognition** check box to enable the function, and then select the alarm object. Select **Person** or **Vehicle**, and then the alarm can only be triggered if the target is person or vehicle. If you disable this function, then the alarm can be triggered by any moving object such as human, vehicle, cat, or dog.  This function is only available on devices with perimeter protection function.
Record Channel	Select **Record Channel**, then click the **Setting** at the right side to select the video stream, and then click **OK**. The system records video for the selected stream when alarm is triggered.  To use this function, you need to enable alarm record and configure auto record first, see the detailed operation in the IPC web operation manual.
Post-Record	The record keeps running for the defined time after alarm is ended.
Alarm Out	Select the connected alarm device such as flashing light or siren, and then the NVR will send alarm signal to them when the alarm is triggered.
Latch	The alarm device keeps running for the defined time after the alarm is ended, and the time rang is from 0 s to 300 s.
PTZ Activation	Select the check box to enable this function, and then click the **Setting** at the right side to select the video stream and PTZ operation. If the alarm is triggered, the PTZ that connected to the selected video stream would perform the defined operation. For example: The PTZ that connected to channel D1 turns to preset 2 when the alarm is triggered.  ● You can only select preset operation for tripwire detection. ● For the PTZ configuration, see the user's manual.

Parameter	Description
Tour	Select the check box to enable this function, and then click the **Setting** at the right side to select the video streams you need, and if the alarm is triggered, the NVR will display the selected video streams in turn. ● For the tour configuration, see the user's manual. ● When the tour is finished, the live interface will recover.
Snapshot	Select the check box to enable this function, and then click the **Setting** at the right side to select the video streams you need, and if the alarm is triggered, the NVR will take snapshot for the selected video streams. For the snapshot configuration, see the user's manual.
Voice Prompts	Select the check box to enable this function, and then select the audio file you need at the **File Name** list. If the alarm is triggered, the NVR will play the selected audio file. For the audio file configuration, see the user's manual.
Send email	Select **Send Email**, and when alarm is triggered, the system sends email to the specified mailbox. To use this function, you need to configure Email first. See the user's manual.
Alarm Upload	Select **Alarm Upload**, and when alarm is triggered, the system uploads alarm signal to the network (alarm center). For the alarm center configuration, see the user's manual.
Buzzer	Select **Buzzer**, and when alarm is triggered, the NVR buzzes.
Log	Select **Log**, and when alarm is triggered, the system makes alarm record in the log.

Step 7 Click **OK**.

5.4.4.3 Intrusion

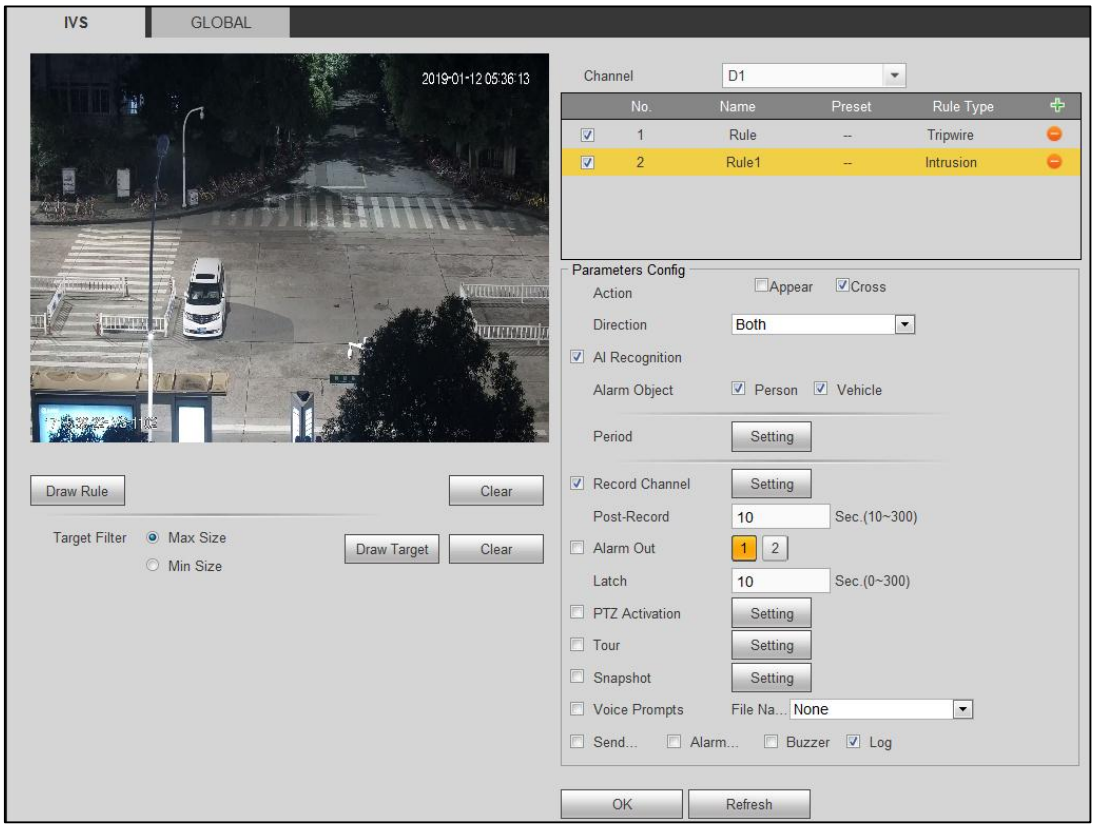
The alarm will be triggered if any target enters, exits, or appears in the defined area.

Step 1 Select **SETUP > EVENT > IVS > IVS**.

The **IVS** interface is displayed.

Step 2 Select the video stream in which you need to configure the rule with its channel No., and then click to add a rule. Double click the words at **Name** column to input the rule name; double click the value at **Rule Type** column, and then select **Intrusion**. See Figure 5-6.

Figure 5-6 Intrusion



Step 3 Click **Draw Rule**, and then draw the area in the image, right click to finish drawing.

Step 4 It requires certain time and moving space for the target to be confirmed, so leave some space outside the area.

Click **Clear** to delete the existing area.

Step 5 Select **Max Size** or **Min Size** at **Target Filter**, and then click **Draw Target** to draw the box.

- Only the targets with the size between **Max Size** and **Min Size** are valid.
- Select **Max Size** or **Min Size** at **Target Filter**, and then click the **Clear** at the right side of **Draw Target** to delete the box.

Step 6 Configure intrusion parameters, for the detailed description, see Table 5-2.

Table 5-2 Intrusion parameter description

Parameter	Description
Working period	Configure working period, and the rule takes effect only within this period. 1. Click **Setting** at **Period**, and then the period setting interface is displayed. 2. Configure each period. • A: Press and hold the left mouse button, and then drag at the periods you need. • B: Click the **Setting** behind the week day you need, and then the week day in the period setting box shows red color, select and configure the periods you need, and you can configure 6 periods in one week day at most. 3. Click **OK**.
AI Recognition	Select the **AI Recognition** check box to enable the function, and then select the alarm object. Select **Person** or **Vehicle**, and then the alarm can only be triggered if the target is person or vehicle. If you disable this function, then the alarm can be triggered by any moving object such as human, vehicle, cat, or dog. This function is only available on devices with perimeter protection function.
Action	Configure intrusion action, you can select **Appear** or **Cross**. • **Appear**: The alarm will be triggered if the target appears in the defined area. • **Cross**: The alarm will be triggered if the target enters or exits the defined area.
Direction	This parameter is displayed only when the **Cross** is selected at **Action**. Configure the intrusion direction, you can select from **Entry**, **Exit** and **Both**.
Record Channel	Select **Record Channel**, then click the **Setting** at the right side to select the video stream, and then click **OK**. The system records video for the selected stream when alarm is triggered. To use this function, you need to enable alarm record and configure auto record first, see the detailed operation in the IPC web operation manual.
Post-Record	The record keeps running for the defined time after alarm is ended.
Alarm Out	Select the connected alarm device such as flashing light or siren, and then the NVR will send alarm signal to them when the alarm is triggered.
Latch	The alarm device keeps running for the defined time after the alarm is ended, and the time rang is from 0 s to 300 s.

Parameter	Description
PTZ Activation	Select the check box to enable this function, and then click the **Setting** at the right side to select the video stream and PTZ operation. If the alarm is triggered, the PTZ that connected to the selected video stream would perform the defined operation. For example: The PTZ that connected to channel D1 turns to preset 2 when the alarm is triggered. ● You can only select preset operation for tripwire detection. ● For the PTZ configuration, see the user's manual.
Tour	Select the check box to enable this function, and then click the **Setting** at the right side to select the video streams you need, and if the alarm is triggered, the NVR will display the selected video streams in turn. ● For the tour configuration, see the user's manual. ● When the tour is finished, the live interface will recover.
Snapshot	Select the check box to enable this function, and then click the **Setting** at the right side to select the video streams you need, and if the alarm is triggered, the NVR will take snapshot for the selected video streams. For the snapshot configuration, see the user's manual.
Voice Prompts	Select the check box to enable this function, and then select the audio file you need at the **File Name** list. If the alarm is triggered, the NVR will play the selected audio file. For the audio file configuration, see the user's manual.
Send email	Select **Send Email**, and when alarm is triggered, the system sends email to the specified mailbox. To use this function, you need to configure Email first. See the user's manual.
Alarm Upload	Select **Alarm Upload**, and when alarm is triggered, the system uploads alarm signal to the network (alarm center). For the alarm center configuration, see the user's manual.
Buzzer	Select **Buzzer**, and when alarm is triggered, the NVR buzzes.
Log	Select **Log**, and when alarm is triggered, the system makes alarm record in the log.

Step 7 Click **OK**.

5.5 Configuring DSS Express

5.5.1 Preparation

- For first time, see the DSS Express user's manual to do initialization and configure IP address and working period. For the hardware requirement, see Table 5-3.
- For the DSS Express that has properly configured, be sure to update the system to the latest version.

Table 5-3 Hardware requirement

Parameter	Hardware requirement
Recommended Configuration	CPU: Intel® Xeon® CPU E3-1220 v5 @3.00GHz RAM: 8GB Ethernet card: 1Gbps Free space: No less than 500Gb
Minimum Configuration	CPU：i3-2120 RAM: 8GB Ethernet card: 1Gbps Free space: No less than 200Gb

5.5.2 Installing DSS Client

You can configure DSS Express through PC client or mobile app, this guide takes PC client for example.

System requirement

Table 5-4 System requirement

Parameter	System requirement
Recommended Configuration	CPU：i5-6500 Clock speed: 3.20GHz RAM: 8GB Graphic card: Intel® HD Graphics 530 Ethernet card: 1Gbps Free space: No less than 100Gb
Minimum Configuration	CPU：i3-2120 RAM: 4GB Graphic card: Intel（R）Sandbridge Desktop Gra Ethernet card: 1Gbps Free space: No less than 50Gb

Operation

Step 1 Open network explorer, and then enter the IP address of the DSS Express at the address bar, and then click 

to download the client.

Click 

, and then scan the QR code with your phone to download the mobile app.

Step 2 Install the program as instructed.

Step 3 Run the client, then input user name, password, IP address, and HTTPS port, and then click **Login**.

User name and password are what you configured during initialization, and the HTTPS port is 443 by default.

5.5.3 Add device

You can add cameras or NVR with auto scan, manual search or batch import. This guide takes manual search for example. See other operations at the DSS Express user's manual.

You need to edit the existing user information and permit them to use the newly added devices.

Step 1 Login the DSS Client.

The home page is displayed.

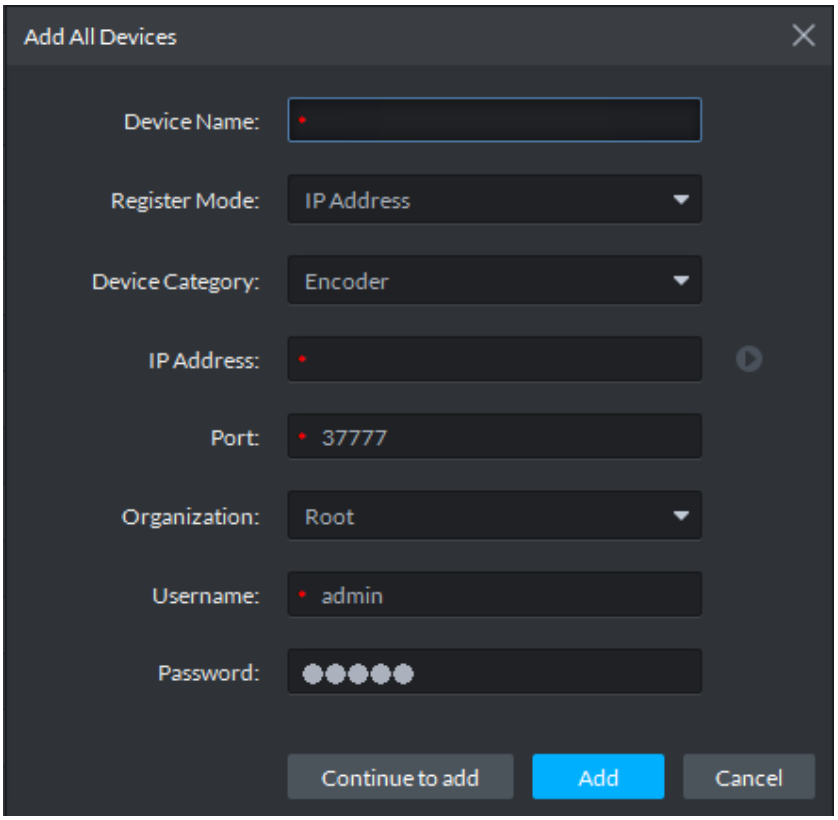
Step 2 Click **Device**.

The **Device** interface is displayed.

Step 3 Click **Add**.

The **Add All Device** interface is displayed. See Figure 5-7.

Figure 5-7 Manual search



Step 4 Configure parameters. See Table 5-5.

- If you add cameras to the DSS Client, then you can manage cameras on the DSS Client directly.
- If you add NVR to the DSS Client, then you can manage cameras on the DSS Client through NVR.

Table 5-5 Parameter description

Parameter	Description
Device name	It is recommended to name devices with the monitoring area for easy identification.
Device Category	Select the device type you need.

Parameter	Description
IP Address	Input the IP address of the target device.
Port	Transmission control protocol port, the value is 37777 by default.
Organization	Select the organization that the target device belongs to.
User Name	Input the user name/password of the device you need.
Password	

Step 5 Click **Add**.

If you need to add more devices, click **Continue to Add** to stay at this interface.

5.5.4 Configuring Alarm

You can configure the way how the alarms are displayed, including alarm sound or flashing on the map.

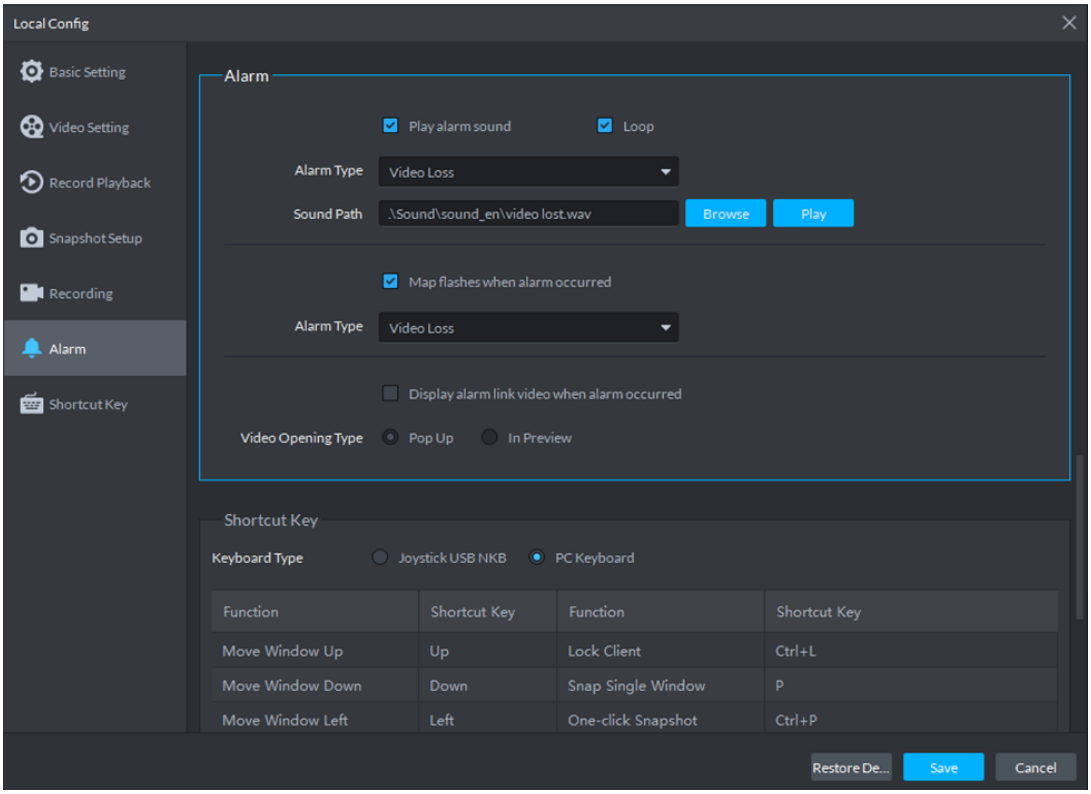
Step 1 Login the DSS Client, and then click .

The **LocalConfig** interface is displayed.

Step 2 Click **Alarm**.

The **Alarm** interface is displayed, see Figure 5-8.

Figure 5-8 Alarm



Step 3 Configure parameters. See Table 5-6.

There will be system notifications when the alarms are triggered.

Table 5-6 Alarm parameter description

Parameter	Description
Play alarm sound	The client will play alarm sound when the alarm is triggered, you can

Parameter	Description
Loop	import audio files and configure different sounds for different alarm types.
Alarm Type	
Sound Path	
Map flashes when alarm occurred	The alarm position on the map will flash when the alarm is triggered. You can select from Video Loss, External Alarm, Moving Detection, video Tampering, and Disconnection.
Alarm Type	
Display alarm link video when alarm occurred	The linked live interface is displayed when the alarm is triggered. You can select pop up or open on the live interface.
Video Opening type	

Step 4 Click **Save**.

5.5.5 Configuring Alarm Events

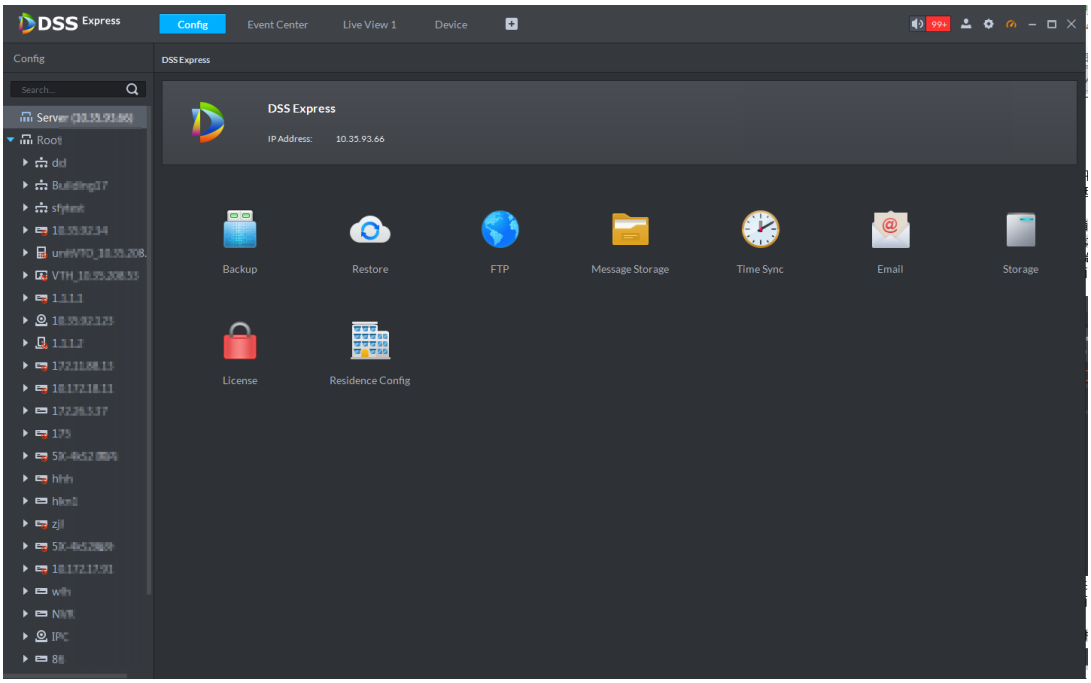
The NVR or IPC will send all the alarms, and the DSS Client only responds to the alarms that are enabled. The supported alarm types vary with different NVR or IPC, but the event parameters are universal.

You need to configure every alarm type.

Step 1 Login the DSS Client, and then click **Config**.

The **Config** interface is displayed, see Figure 5-9.

Figure 5-9 Config



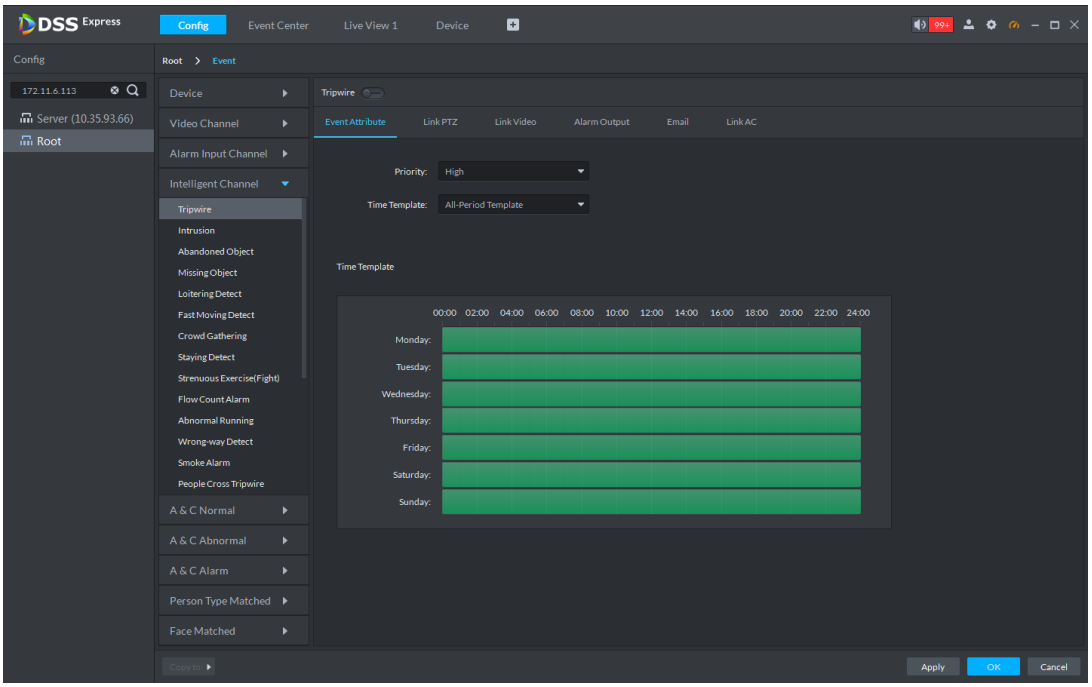
Step 2 Select a device or a video stream from the list at the left side, and then click **Event Config**.

The **Event** interface is displayed. Click **Root**, and then the event configuration of the selected device is displayed.

Step 3 Select **Tripwire** or **Intrusion** at **Alarm Type**.

The **Event Attribute** interface is displayed, see Figure 5-10.

Figure 5-10 Event



Step 4 Click  to enable this event.

 means it is enabled, and then the  is displayed behind this event in the list.

Step 5 Configure alarm linkage

- Event Attribute: Select priority for the event, and then configure working period.
- Link PTZ: Select PTZ from the device list. Click the drop down list, and then select the preset. The PTZ turns to the selected preset when the alarm is triggered.
- Link Video: Select a window, and then drag the selected device or stream in the window, the device or stream is displayed in the list. You can configure storage path, stream type, record time, or take snapshot or play video when the alarm is triggered.
- Alarm Output: Select the alarm device you need. Click the alarm duration list to select the duration you need. 当产生报警时，系统会联动选定的报警输出。
- Email: Input target mail address, or click address, and then select the address you need and input mail title. You can configure mail content or input the content as needed. Example: Select **Event Time**, and the event time will be included in the mail content.
- Link AC: Select the access control device you need. The linkage action is displayed. There are unlock, lock, NO, and NC.

Step 6 Click **Save**.

5.6 Configuring DMSS Client

5.6.1 Preparation

- Make sure to obtain the compatible DMSS Client.

- Make sure the mobile phone that installed DMSS Client is in the same network as the NVR.

5.6.2 Installing DMSS Client

You can operate and configure devices on the DMSS Client.

Mobile phone system requirement

Table 5-7 System requirement

Parameter	System requirement
Android	Android 4.4 or above. Push service is available only when you installed plus version and use Google account.
iOS	iOS 8.0 or above.

Operation

This guide takes iOS for example.

Step 1 Search and download iDMSS Plus from App Store.

Step 2 Tap  to run the client.

- Select the region as needed.
- The **Live Preview** interface is displayed, see .

Step 3 Tap  >  , and then the login interface is displayed.

Step 4 Input mail box and password, and then tap **Login**.

You can login with Imou account.

You can also login with Imou account.

5.6.3 Add device

You can add cameras or NVR with or without wire, and you can add devices within the same LAN.

See the DMSS user's manual for initialization.

This guide takes adding cameras or NVR with wire for example. See the DMSS user's manual for wireless operation.

Step 1 Login DMSS client

The home page is displayed.

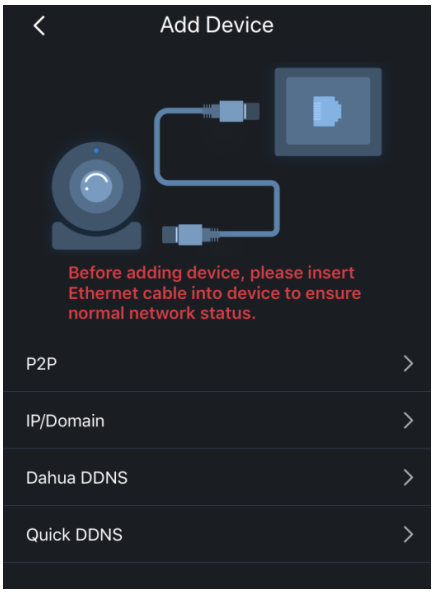
Step 2 Tap  > **Device Management** >  > **Remote Monitor**.

The **Add Device** interface is displayed.

Step 3 Tap **Wired Device**.

The **Add Device** interface is displayed. See Figure 5-11.

Figure 5-11 Add device



Step 4 Select adding method, and then configure parameters. See Table 5-8.

- If you add cameras, then you can manage cameras on the DMSS client directly.
- If you add NVR, then you can manage cameras on the DMSS client through NVR.

Table 5-8 Parameter description

Parameter	Description
Name	Input the name of the device.
SN	The SN is needed if you select **P2P**. You can input manually or scan the QR code to get the SN.
Address	• If you select IP/Domain, then input the IP address or domain name. • If you select Quick DDNS or Dahua DDNS, input the DDNS domain.
Port	The port is needed if you select IP/Domain. It is 37777 by default.
User Name	Input the user name/password of the device you need.
Password	
Live preview	Select **Main Stream** or **Sub Stream** for live video.
Playback	Select **Main Stream** or **Sub Stream** to record and playback.

Step 5 Click **Start Preview**.

The live video is displayed.

5.6.4 Subscribing Alarm

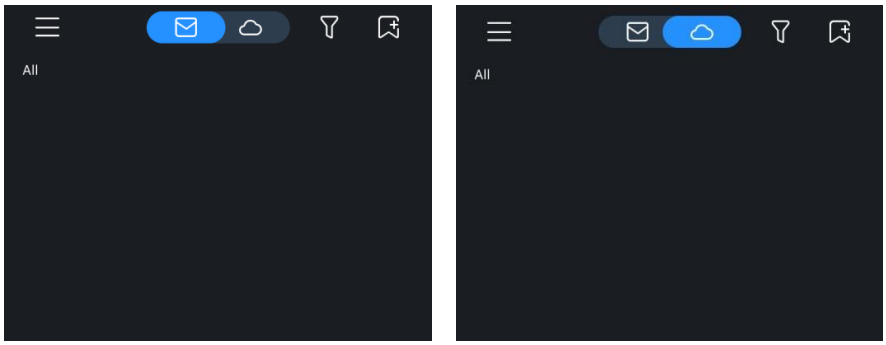
You need to subscribe alarm, and then the camera or NVR will push alarms to your mobile client. You can subscribe alarms of local devices and remote devices.

This guide takes subscribing tripwire for example.

Step 1 Tap ☰ > Messages.

The **Messages** interface is displayed, see Figure 5-12. The local alarm interface is displayed by default, and you can tap  to see remote alarm interface.

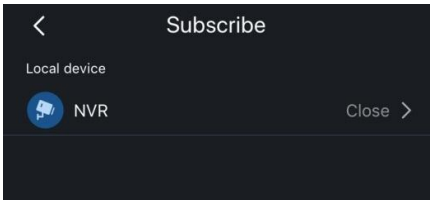
Figure 5-12 Messages.



Step 2 Tap  .

The device list is displayed. See Figure 5-13.

Figure 5-13 Enable subscribe



Step 3 Select the device from which you need alarms, and then tap  .

The subscribe configuration is displayed, see Figure 5-14.

Figure 5-14 Subscribe configuration

Step 4 Tap IVS > Cross Line, and then select the video stream. See Table 5-9.

You can subscribe multiple alarms.

Table 5-9 Subscribe configuration description

Parameter	Description
Push Type	You can select from **Live Preview**, **Video**, and **Snapshot**. ● Live Preview: The DMSS client will receive live video when the alarm is triggered. ● Video: If video recording is enabled on the camera or NVR, the DMSS client will receive and play the alarm recording when the alarm is triggered. ● Snapshot: If snapshot is enabled on the camera or NVR, the DMSS client will receive and play the alarm snapshot when the alarm is triggered.
Alarm Type	You can select the alarm type as needed. ● IVS: Including tripwire, intrusion, abandoned object,missing object, and scene changing. ● Thermal Imaging: This alarm is triggered when there is abnormal temperature change in the image. There are 6 alarm modes, including temperature alarm, temperature difference alarm, fire alarm, high temperature spot alarm, low temperature spot alarm, and human fever alarm. This alarm type requires thermal imaging camera. ● Motion Detect: This alarm is triggered when there is abnormal moving object in the image. It includes human detection and motion detection. ● Cam Masking: This alarm is triggered when the camera is covered and cannot collect image. ● Defocus: This alarm is triggered when the camera cannot focus on the target or has soften or blur image. ● Face Alarm: This alarm detects human faces in the image and makes alarm under defined conditions. ● Audio Detect: This alarm detects sound in the video and makes alarm under defined conditions. ● HDD Alarm: This alarm is triggered when there is no disk, disk is full, or disk error. ● Power Detect: This alarm is triggered when the device voltage is too low or too high. ● Network Alarm: This alarm is triggered when the camera is offline. ● Sensor Alarm: This alarm is triggered when there is alarm information from the connected sensors.

Step 5 Tap .

5.7 Commissioning

5.7.1 DSS Express Commissioning

5.7.1.1 Live

After the IVS rules are properly configured, the rule box is displayed on the live interface with blue color, and it flashes with red color when the alarm is triggered.

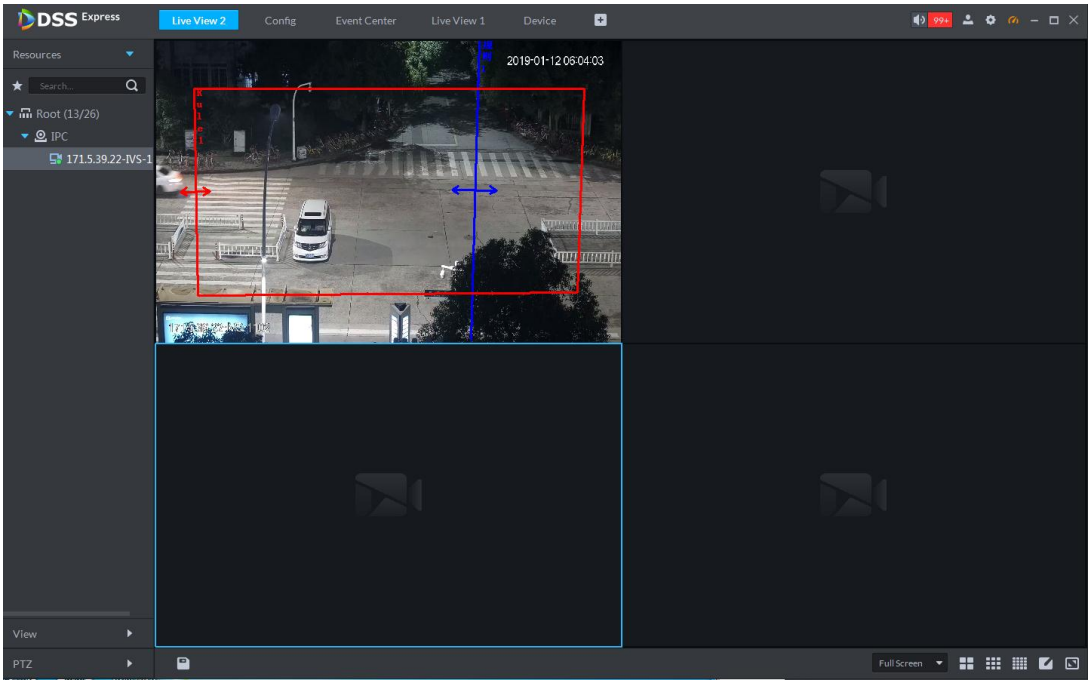
Step 1 Login the DSS Client, and then click **Live View**.

The **Live View** interface is displayed.

Step 2 Double click a video stream or drag it with the mouse to put it in the window.

The live video and defined rule box are displayed. See Figure 5-15.

Figure 5-15 Live video

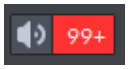


5.7.1.2 Processing Alarms

The client will receive alarm message when any alarm is triggered.

Step 1 Login the DSS Client, and then click **Event Center**.

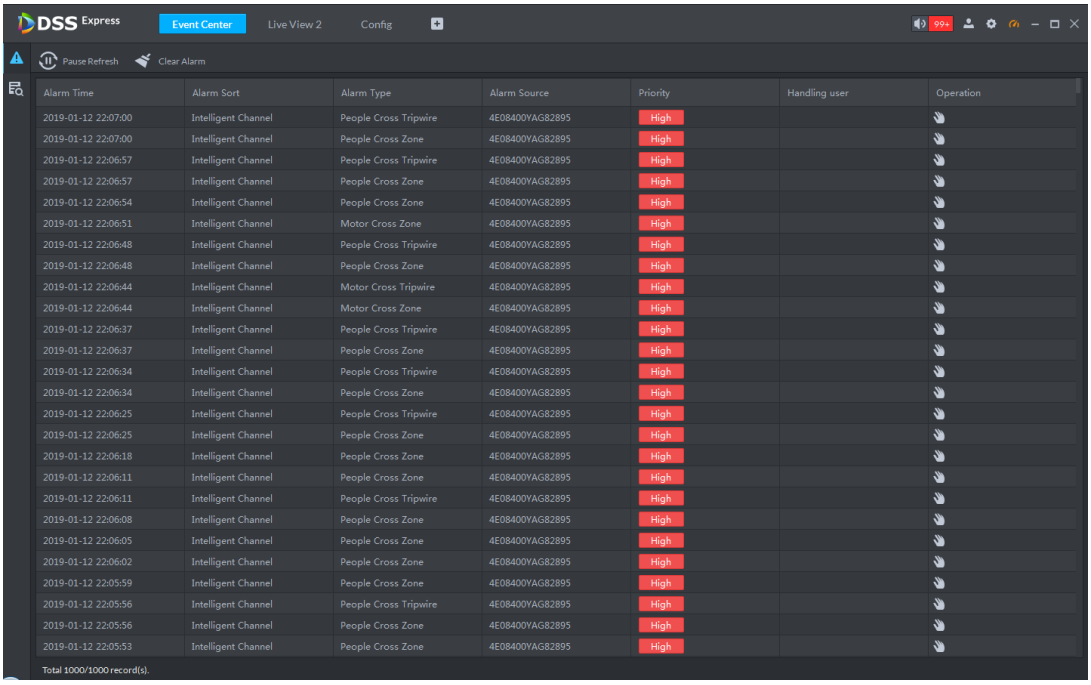
The **Event Center** interface is displayed.

Step 2 Click **Event Center** or the 

at the upper right corner of the interface.

The **Event** interface is displayed, see Figure 5-16.

Figure 5-16 Event



Step 3 You can process the alarm with the following methods.

1) Select an alarm, and then click  .

   The icon changes to  , which means the user has confirmed the alarm, and the user name is displayed at the **Handing user** column.

2) Click  .

   The alarm processing interface is displayed.

3) You can click tabs including Information, Live, Snapshot, Recording, or Map to view the alarm details.

4) You can process the alarm with the following methods.

   ◇ Input your opinion.

   ◇ Forward to other users.

   ◇ Dismiss, and do not show the same alarm within the defined period.

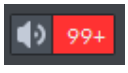
   ◇ Send email.

5.7.1.3 Viewing Alarm History

You can view all the alarms in the log.

Step 1 Login the DSS Client, and then click **Event Center**.

The **Event Center** interface is displayed.

Step 2 Click **Event Center** or the 

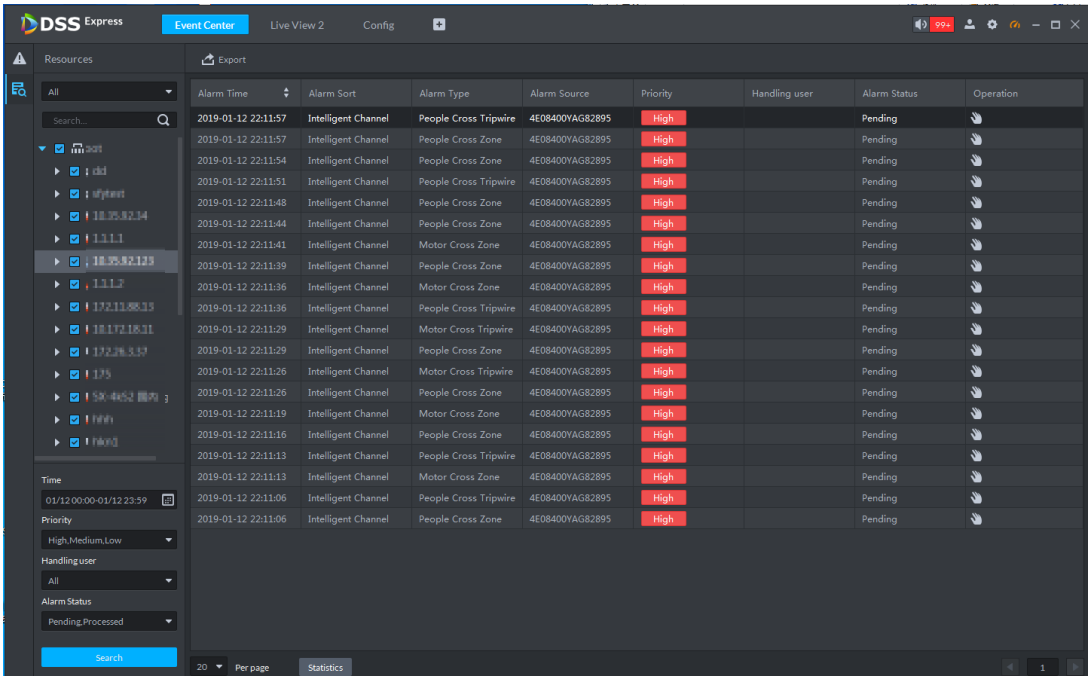
at the upper right corner of the interface.

The **Event** interface is displayed, see Figure 5-16.

Step 3 Click  .

The alarm history is displayed, see Figure 5-17.

Figure 5-17 Alarm history



Step 4 Configure search conditions, and then click **Search**.

The search result is displayed. You can only search alarms within the same month.

Step 5 You can process the alarm with the following methods.

Step 6 You can also export the alarm history.

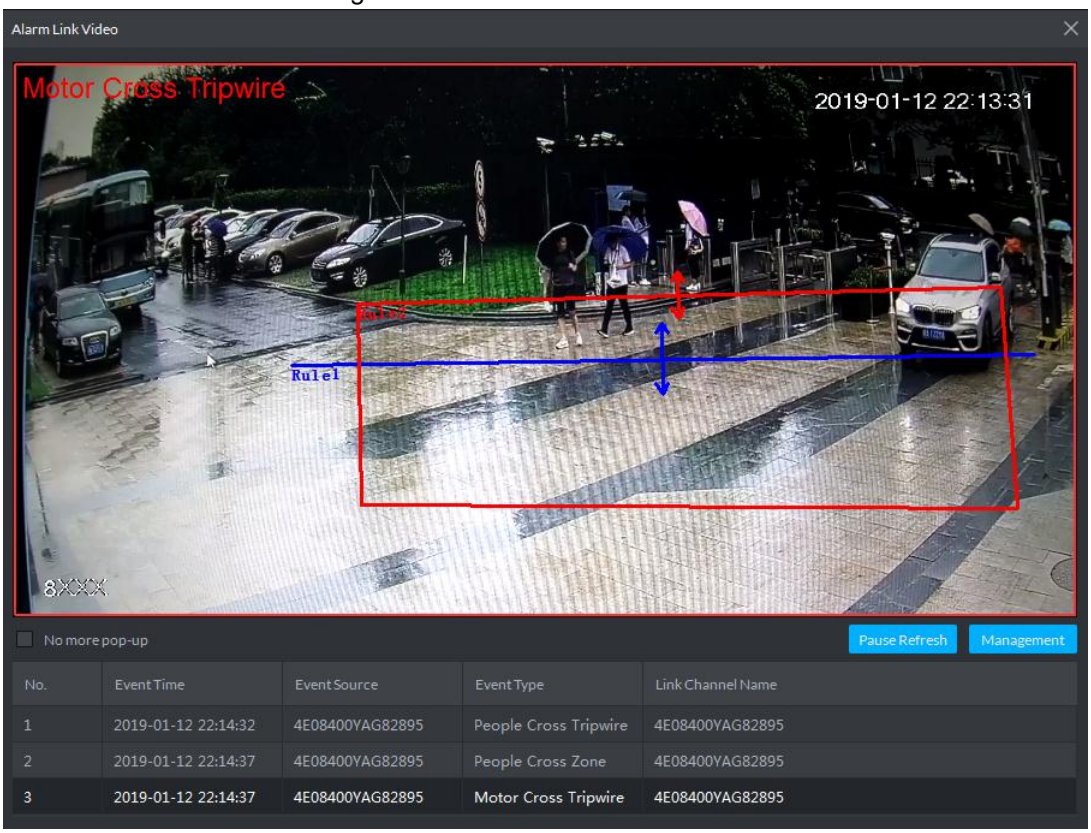
5.7.1.4 Alarm Link Video

Configure alarm link video and enable auto play, and then the system will play the live video when the alarm is triggered.

You can perform the following operations on the **Alarm Link Video** interface. See Figure 5-18.

- View alarm time, object type and video channel information.
- Select **No more pop-up**, and then the video window will not pop up anymore.
- Click **Pause Refresh**, and then the alarm is paused.
- Click **Management**, and then the alarm processing interface is displayed.

Figure 5-18 Alarm link video



5.7.2 DMSS Commissioning

5.7.2.1 Live preview

You can view the added live videos, record video, take snapshot, or configure video image.

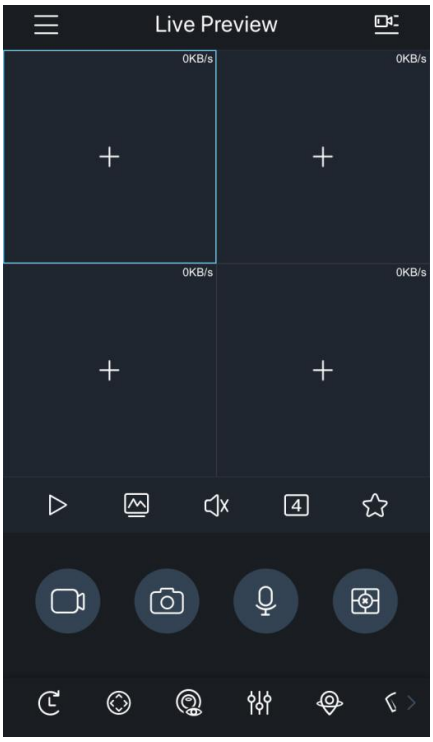
Step 1 Login DMSS client

The home page is displayed.

Step 2 Tap > **Live Preview**.

The **Live Preview** interface is displayed, see Figure 5-19.

Figure 5-19 Live preview



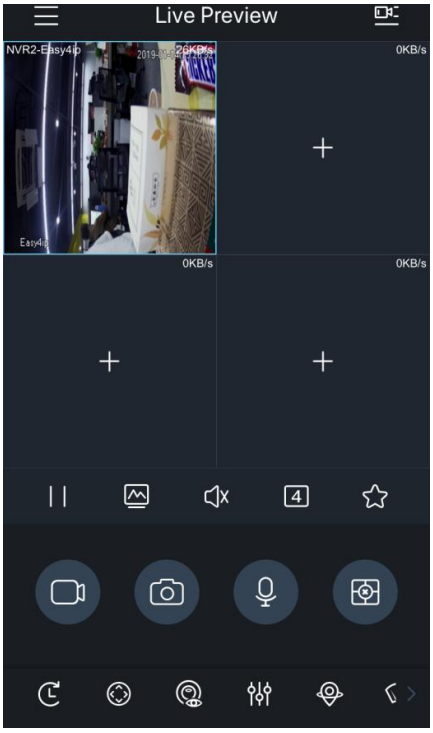
Step 3 You can perform the following operations:

- Tap  to select and play the video stream you need.
- Tap  , then select one or multiple video streams, and then tap **Start Preview** to play the selected videos.

  There are 4 windows by default, and if you select more than 4 video streams, there will be more windows displayed. Swipe left or right to view different videos.
- Tap  to play the most recent video.

The video bit rate is displayed at the upper right corner of the window. See Figure 5-20.

Figure 5-20 Live preview

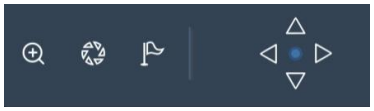


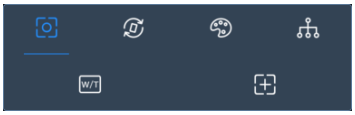
You can tap the buttons to perform more operations. Swipe left or right at the bottom tool bar to get more buttons. See Table 5-10. 滑动底部工具栏，可选择更多功能。

Table 5-10 Button Description

Button	Description
	Select a video, and then tap to pause, the button changes to . Tap to play.
	Select a video, and then tap to select the stream type you need. The button changes to blue color, which means the operation succeeded. ● Tap to select sub stream, which is more fluent. ● Tap to select main stream, which has better quality. ● Tap to modify coding parameters as needed.
	Select a video, and then tap to enable sound, the button changes to . Tap to mute.
	Tap to change window quantity. You can display 4, 9, and 16 windows.

Button	Description
	Select a video, and then tap  to add it to your favorite. See more details in the user's manual.
	Select a video, and then tap  to start recording, the button changes to  . Tap  to stop recording. ● During recording, the recording status and duration are displayed on the upper left corner. ● You can manage the recorded videos in the **File Manager**. See more details in the user's manual.
	Select a video, and then tap  to take snapshot. ● You can configure the snapshot quantity on the **Local Config** interface. See more details in the user's manual. ● You can manage the snapshots in the **File Manager**. See more details in the user's manual.
	Select a video, and then tap  to start audio intercom, the button changes to  . Tap  to stop intercom.
	Select a video, and then tap  to playback video from a certain time ago (30 s by default), the button changes to  . Tap  to stop playback. You can configure the playback start time on the **Local Config** interface. See more details in the user's manual.

Button	Description
	Select a video, and then tap to operate PTZ, the button changes to . Tap to exit.  ● Tap to zoom. ● Tap to adjust aperture. ● Tap , then select the preset point, and then to turn the PTZ to the selected point. ● Tap , , , and to turn the PTZ. You can also use gestures to control PTZ. ● Swipe with two fingers on the screen to turn the PTZ. ● Pinch or stretch out with two fingers on the screen to zoom the picture. ● This function is available on PTZ models. ● Only one window is displayed during PTZ control.
	Select a video, and then tap to enable fish eye mode. Tap again to exit. You can swipe on the screen to adjust fish eye effect. This function is only available on fish eye models.

Button	Description
	Select a video, and then tap to configure video image, the button changes to . Tap to exit.  ● Tap to configure focus or zoom. ◇ Tap to focus. ◇ Tap to zoom. ● Tap to rotate or flip the image. ◇ Tap to flip horizontally. ◇ Tap to flip vertically. ◇ Tap to rotate 270°. Tap again to resume. ◇ Tap to rotate 90°. Tap again to resume. ◇ Tap to rotate 180°. ● Tap configure image parameters. ◇ Tap to change brightness. ◇ Tap to change contrast. ◇ Tap to change hue. ◇ Tap to change saturation. ◇ Tap to reset to default. ● Tap to change live video quality. ◇ Tap to select best quality. ◇ Tap to select low quality. ◇ Tap to select adaptive mode.

Button	Description
	Select a video, and then tap  to enable smart tracking. Tap again to exit.
	Tap  , and then the wiper control interface is displayed. ● Tap **Single**, the wiper works one time, and then stop. ● Tap **Enable**, then configure time interval, the wiper works after each time interval. ● Tap **Stop**, the wiper stops working. This function is available on select models.
	Tap  to turn on the light/buzzer on the connected device. Tap again to turn off. This function is available on select models.
	Select a video, and then tap  , the alarm output control panel is displayed. You can enable or disable alarm output. This function is available on models with alarm output function.
Full screen	Hold the phone on the portrait mode, and then the system switches to full screen. Be sure to enable portrait mode on your phone.
Change window	Tap and hold a video, and then you can drag it to the target window.
Enlarge window	Double tap the window to enlarge it. Double tap again to resume.
Open help document	If the video is not properly displayed, tap the **Help** button in the window to see the help document.
Close video	● Close single video: Tap and hold a video, and then drag it to the trash can on the top of the interface. ● Close multiple videos: Tap  to close all the current videos.

5.7.2.2 Processing Alarms

Configure push service properly, and then your mobile client will receive messages if any alarm is triggered.

Tap  , and then select **Messages** to view the alarm messages. The system classifies all alarm messages by different devices, you can select a certain device to view its alarms. See Figure 5-21.

- Alarm messages with red dot on them are not processed.

- Tap  to filter alarm messages.
- Delete alarm device/alarm messages
  - ◇ Android: Tap and hold the alarm device/alarm messages, and then tap **OK**.
  - ◇ iOS: Swipe left on the alarm device/alarm messages, and then tap **Delete**.
- Tap the alarm message, and then the system perform the defined operation at **Push Type**, including open recorded video, snapshot, or live video. See Figure 5-22.

  You need to install storage device and configure video recording on the camera first.

Figure 5-21 Alarm messages

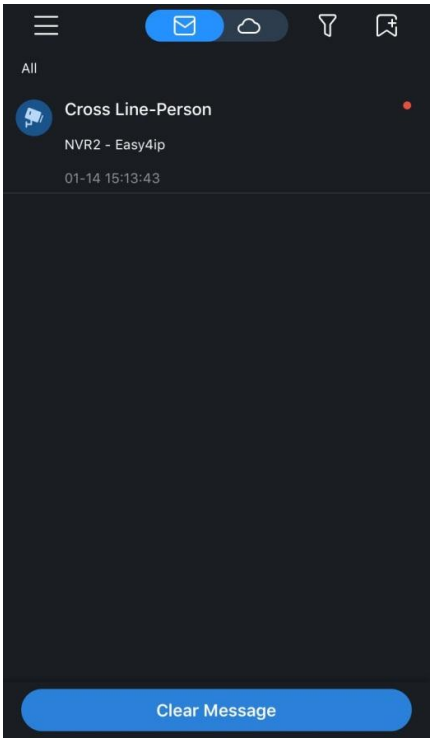
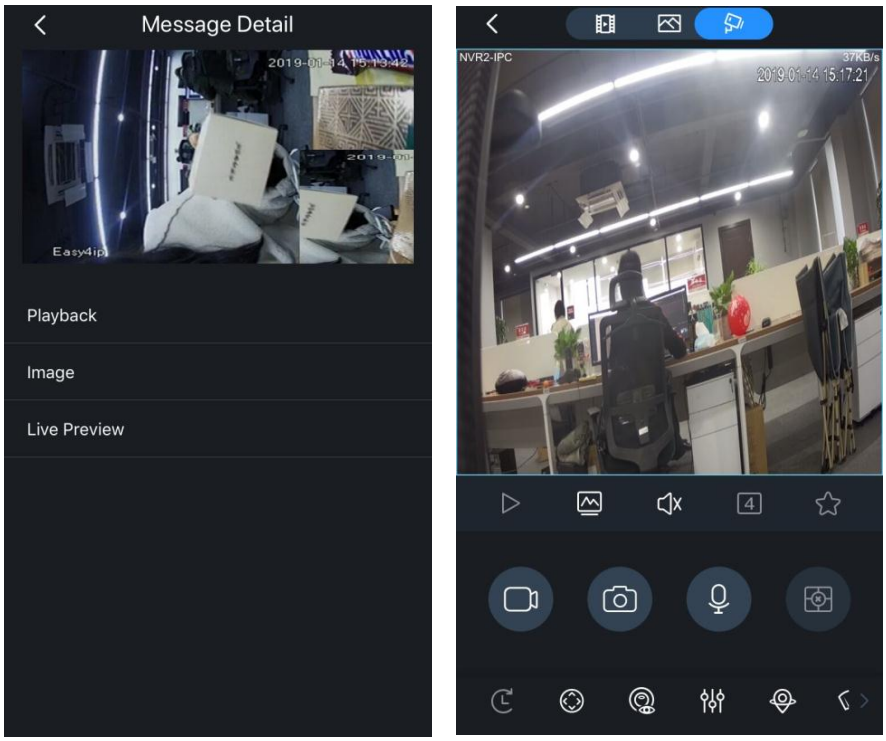


Figure 5-22 Alarm videos



Dahua North America
23 Hubble
Irvine, CA 92618

Tel: (949) 679-7777
Fax: (949) 679-5760
Support: 877-606-1590

Sales: sales.usa@dahuatech.com
Support: support.usa@dahuatech.com
Website: us.dahuasecurity.com