Dahua Thermal Body Temperature Monitoring Solution

Deployment Guide

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD. V2.0.0

Foreword

Safety Instructions

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

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

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	March 2020

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 Manual

- The manual is for reference only. If there is inconsistency between the manual 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 manual.
- The manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.

- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the manual (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please 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 that 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 (CMOS) directly. 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 that 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.

Table of Contents

1 Overview

The solution aims at body temperature monitoring and alarm at various checkpoints such as railway stations, airports and community entrances, and features high precision & reliability, quick temperature recognition rate, easy installation and high cost performance.

The solution adopts thermal network camera (hereinafter referred to as TPC) with the help of blackbody to detect body temperature and send temperature data and alarm to Express, DMSS, IVSS or NVR to notify inspectors.

📖

The deployment guide is for reference only. If there is any difference between the guide and the product, the actual product shall prevail.

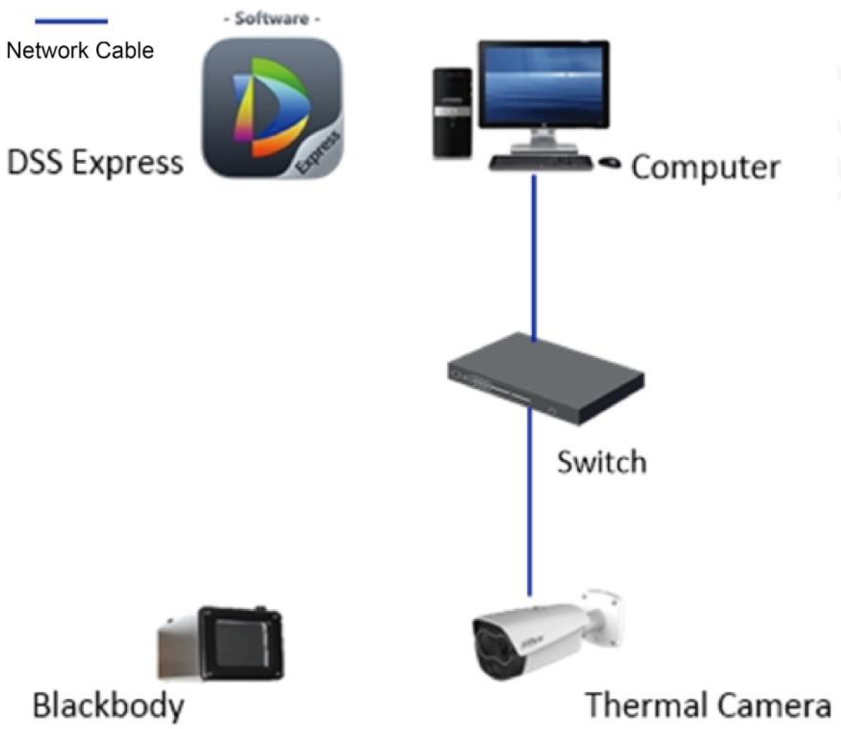
2 Network Diagram

This solution provides the following network diagrams, and you can choose according to your actual needs.

- TPC–Express

  TPC is directly added to Express. Video and pictures are stored in the disks of Express server. Express is used for video and alarm monitoring and system management.

Figure 2-1 TPC–Express



- TPC–IVSS/NVR–Express

  TPC is added to IVSS/NVR; IVSS/NVR is added to Express. Video and pictures are stored in IVSS/NVR. Express is used for video and alarm monitoring and system management.

Figure 2-2 TPC–IVSS–Express

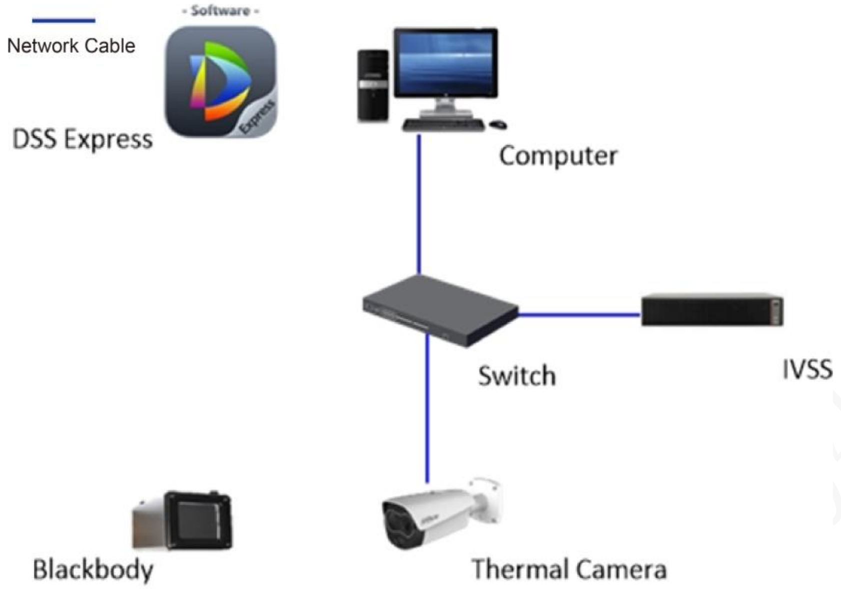
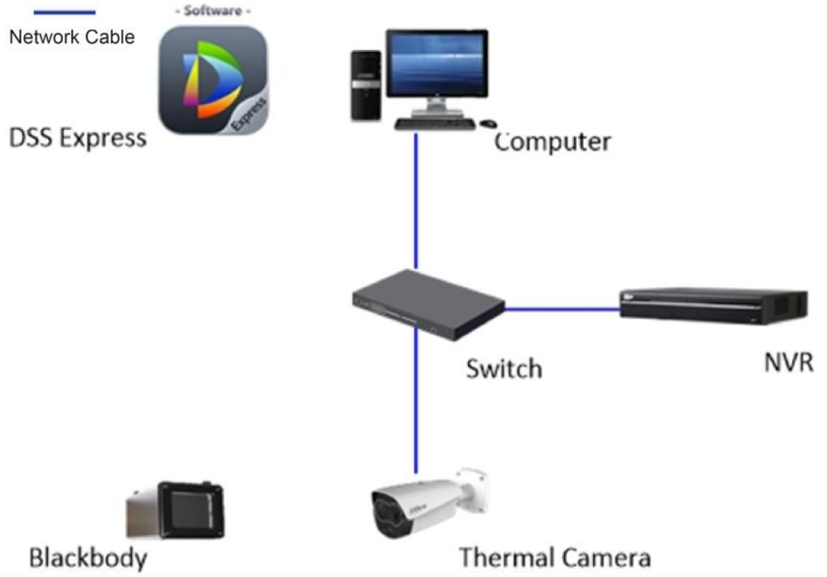


Figure 2-3 TPC–NVR–Express



- TPC–IVSS/NVR

  TPC is added to IVSS/NVR. Video and pictures are stored in IVSS/NVR. Video and alarm monitoring and system management are performed on IVSS/NVR.

Figure 2-4 TPC–IVSS

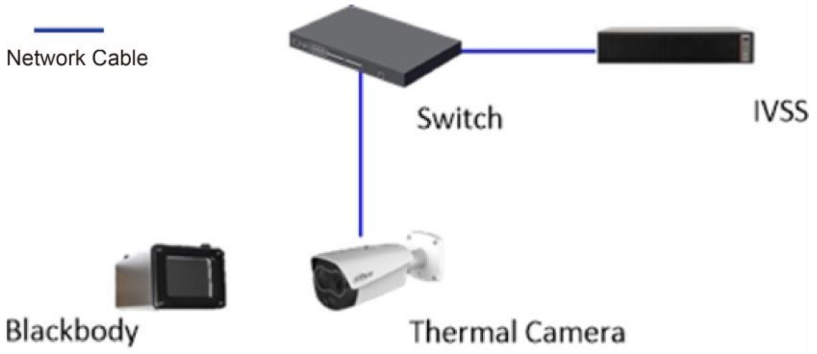
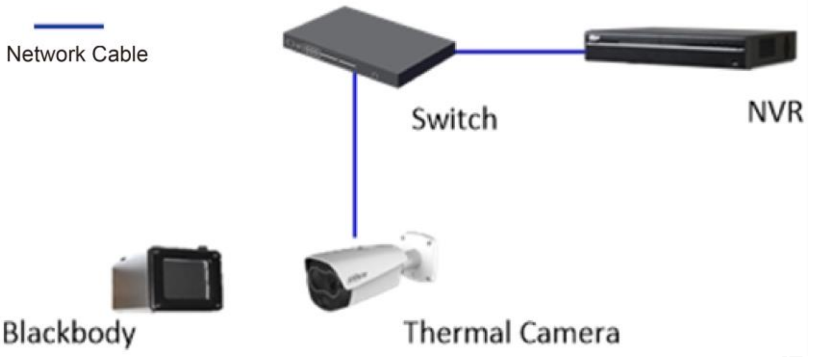
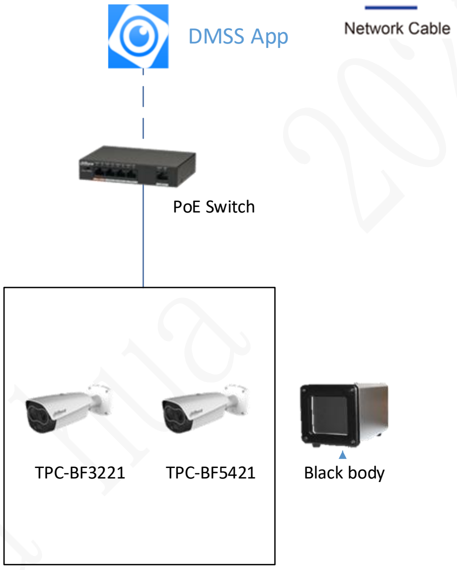


Figure 2-5 TPC–NVR



- TPC–DMSS
  Add TPC to DMSS to live view video image. Store TPC images or video on TPC SD card or DMSS cloud.

Figure 2-6 TPC–DMSS



- TPC–IVSS/NVR–DMSS
  Add TPC to IVSS or NVR, then to DMSS. View video image on IVSS, NVR or DMSS. Store TPC images or video on IVSS, NVR or on DMSS cloud.

Figure 2-7 TPC–IVSS–DMSS

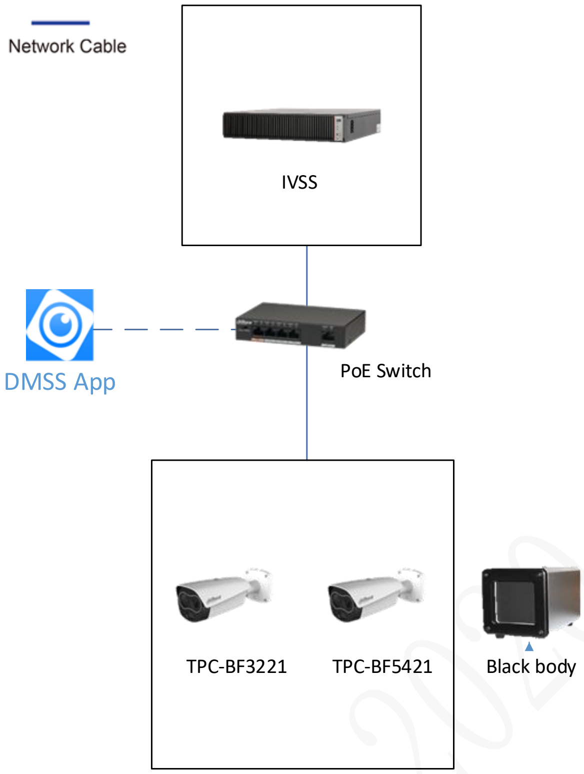
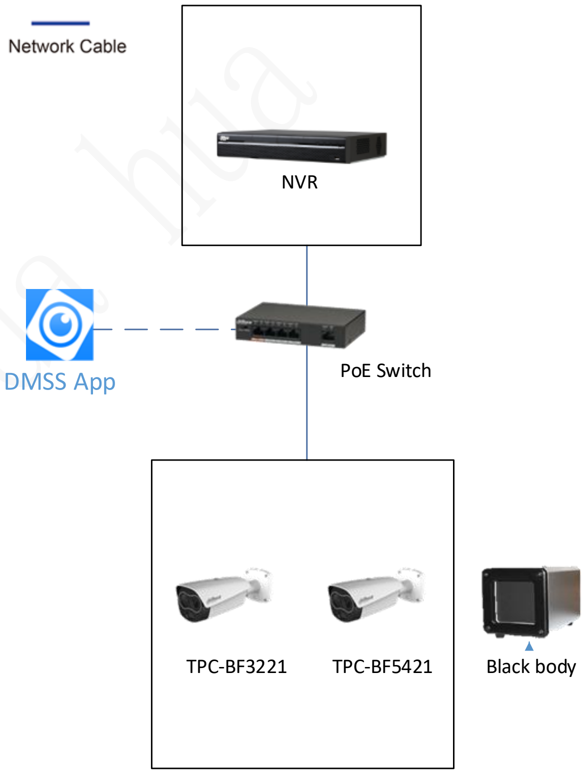


Figure 2-8 TPC–NVR–DMSS



3 Deployment Process

Before deployment, confirm whether all the devices work properly, and then you can start deployment and configuration. You can install all the devices with the provided manual or guide.

Step 1 Confirm the device models and device quantity. For details, see the material list of the solution.

Step 2 Record all the device SN numbers from the packing boxes in Excel.

Figure 3-1 SN number

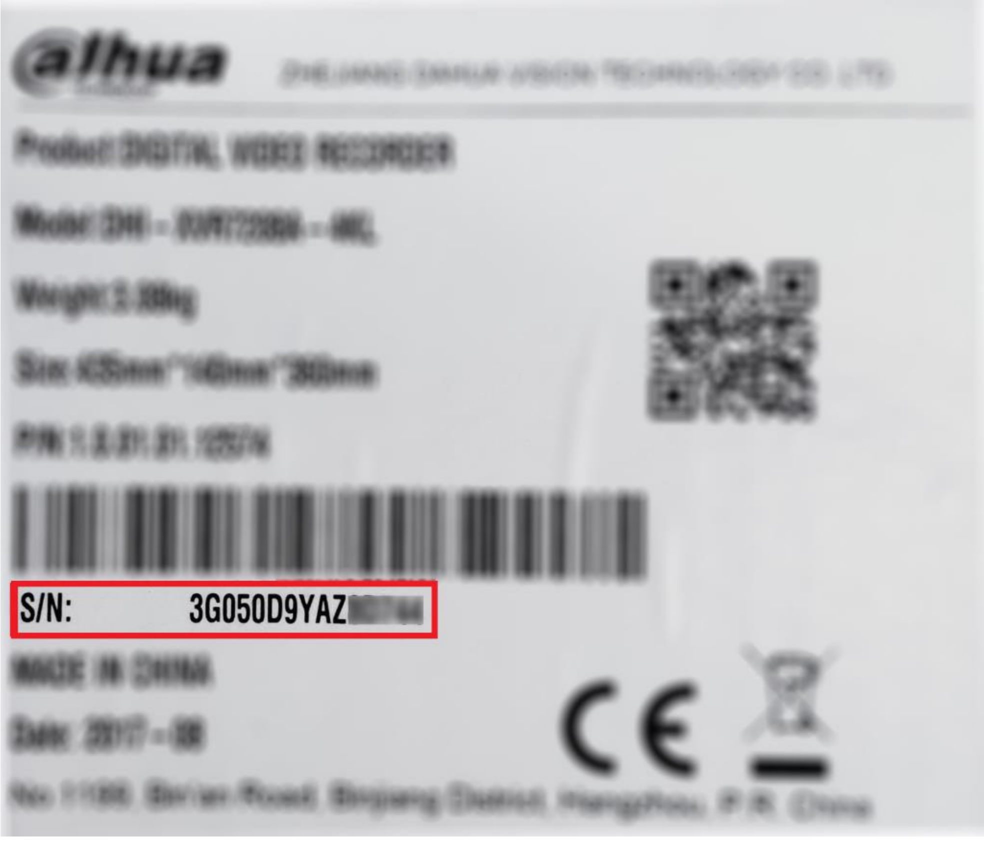
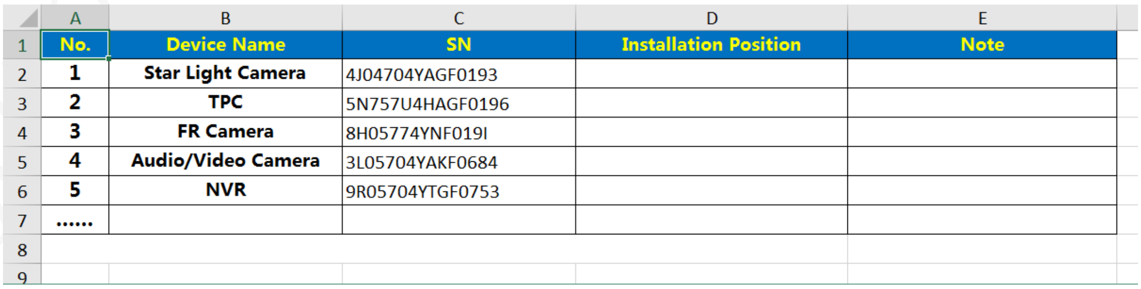


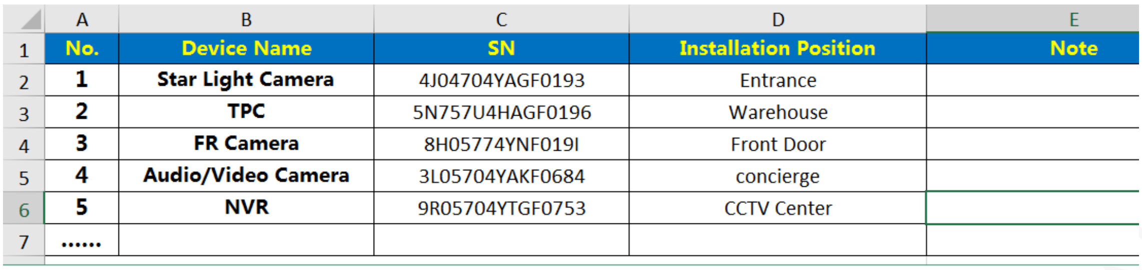
Figure 3-2 Record SN numbers



No.	Device Name	SN	Installation Position	Note
1	Star Light Camera	4J04704YAGF0193		
2	TPC	5N757U4HAGF0196		
3	FR Camera	8H05774YNF019I		
4	Audio/Video Camera	3L05704YAKF0684		
5	NVR	9R05704YTGF0753		
......				

Step 3 Match all the SN numbers with the planned installation positions in the table. You can also modify the content in the table as needed.

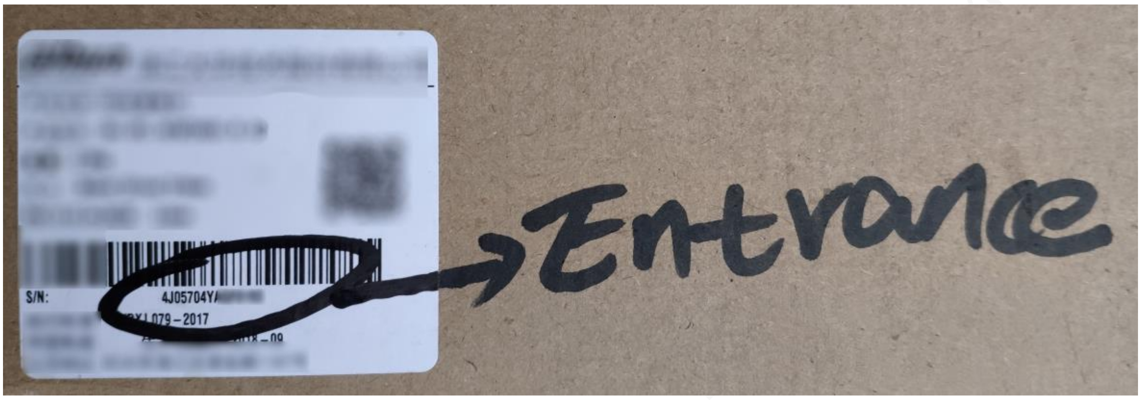
Figure 3-3 Match installation position



No.	Device Name	SN	Installation Position	Note
1	Star Light Camera	4J04704YAGF0193	Entrance	
2	TPC	5N757U4HAGF0196	Warehouse	
3	FR Camera	8H05774YNF019I	Front Door	
4	Audio/Video Camera	3L05704YAKF0684	concierge	
5	NVR	9R05704YTGF0753	CCTV Center	
......				

Step 4 Mark the installation positions on the corresponding packing boxes as planned, and then install them to proper locations. See Figure 3-4 and "4 Installation."

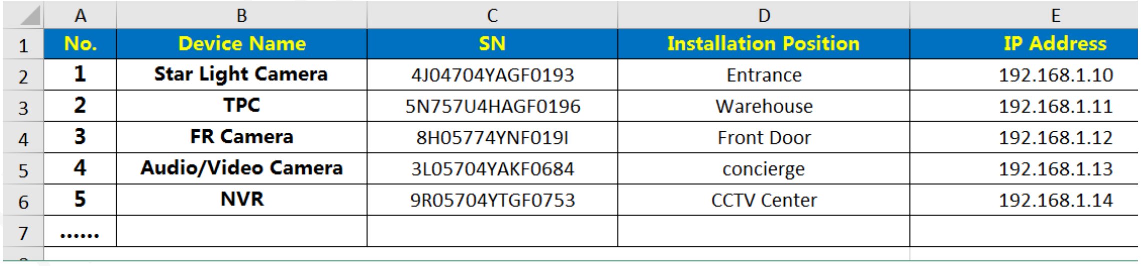
Figure 3-4 Mark installation position



Step 5 Make sure that all the devices are properly connected, and then power up all the devices. Download the ConfigTool on your PC to initialize all the devices and modify device IP addresses in batches. See "5 Getting Started."

Step 6 After modifying all the IP addresses, you can record them to the planning table too, and then you will have the matching relationship between SN number, installation position, and IP address of every device. You can then easily locate every device you need during configuration.

Figure 3-5 Match IP address

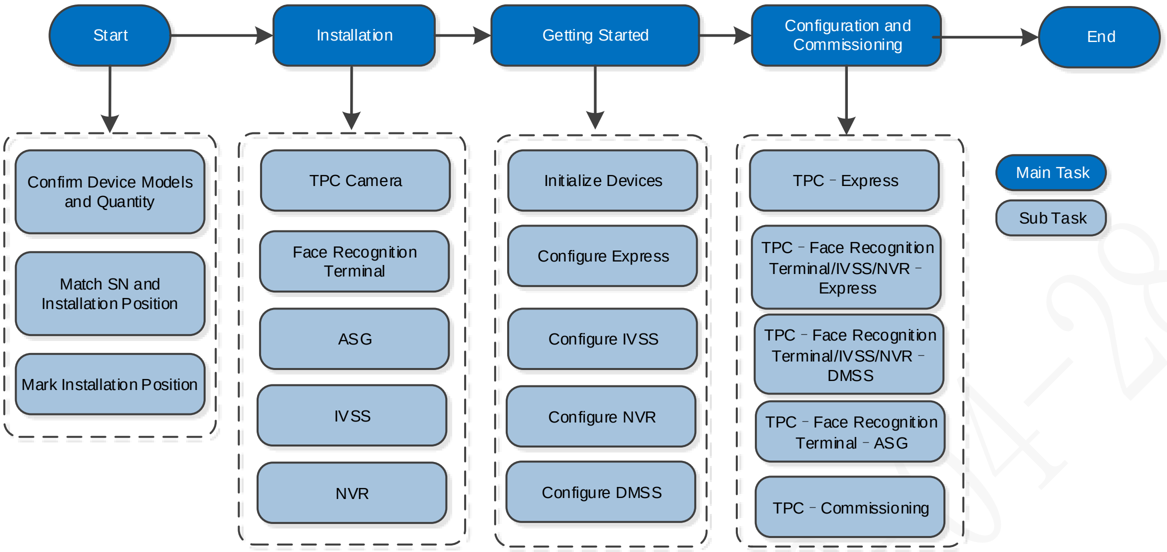


No.	Device Name	SN	Installation Position	IP Address
1	Star Light Camera	4J04704YAGF0193	Entrance	192.168.1.10
2	TPC	5N757U4HAGF0196	Warehouse	192.168.1.11
3	FR Camera	8H05774YNF019I	Front Door	192.168.1.12
4	Audio/Video Camera	3L05704YAKF0684	concierge	192.168.1.13
5	NVR	9R05704YTGF0753	CCTV Center	192.168.1.14
......				

Configure devices and carry out commissioning. See "0

Step 7 Configuration and Commissioning."

Figure 3-6 Deployment


Start
Installation
Getting Started
Configuration and Commissioning
End
Confirm Device Models and Quantity
Match SN and Installation Position
Mark Installation Position
TPC Camera
Face Recognition Terminal
ASG
IVSS
NVR
Initialize Devices
Configure Express
Configure IVSS
Configure NVR
Configure DMSS
TPC－Express
TPC－Face Recognition Terminal/IVSS/NVR－Express
TPC－Face Recognition Terminal/IVSS/NVR－DMSS
TPC－Face Recognition Terminal－ASG
TPC－Commissioning
Main Task
Sub Task

4 Installation and Connection

This chapter introduces connection between TPC and blackbody.

📖

For installation details, refer to products user's manual or quick start guide.

4.1 Installing TPC and Blackbody

4.1.1 Installation Distance

The distance from TPC to forehead should be equal to the distance from TPC to the blackbody to ensure temperature measurement accuracy. Confirm your TPC model and see the table below for specific devices installation distance.

Table 4-1 Devices installation distance

Focal Length	**Distance between TPC and Blackbody**	**Distance between TPC and Body Forehead**	**Width of Passage**
BF3221 (7 mm)	3 m	3 m	1.3 m
BF5421 (13 mm)	3 m	3 m	1.5 m

4.1.2 Installation Illustrations

📖

There is preset factory temperature for blackbody. Blackbody temperature enters its constant state after 30 minutes.

4.1.2.1 TPC (BF3221) and Blackbody

Figure 4-1 Installation (side view)

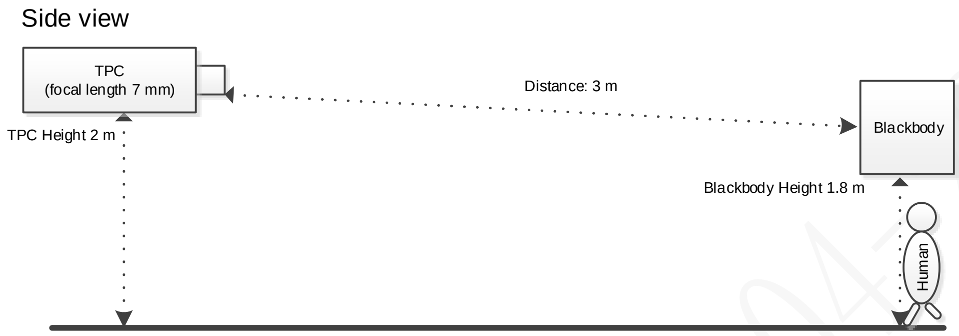
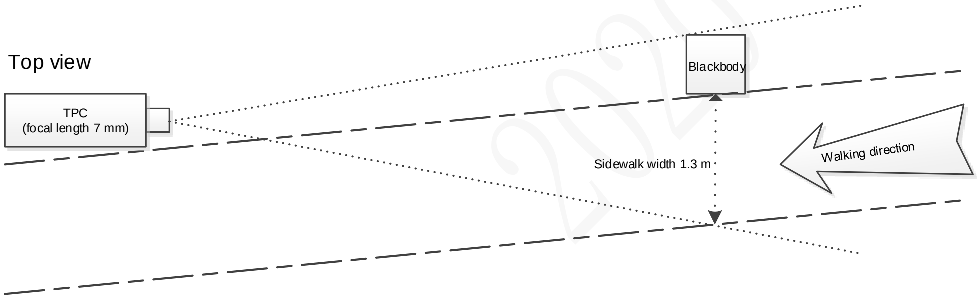


Figure 4-2 Installation (top view)



4.1.2.2 TPC (BF5421) and Blackbody

Figure 4-3 Installation (side view)

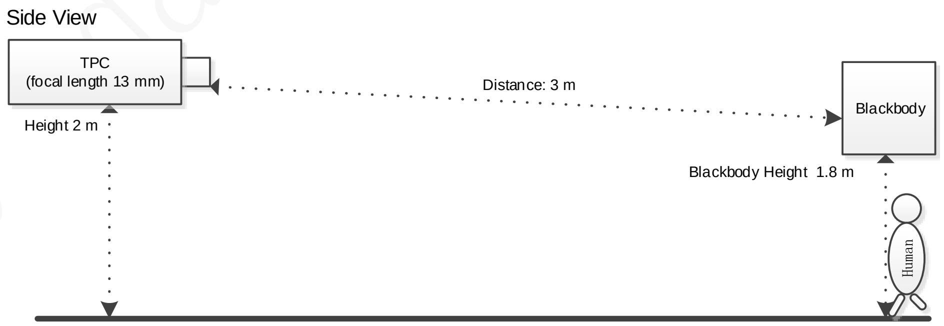
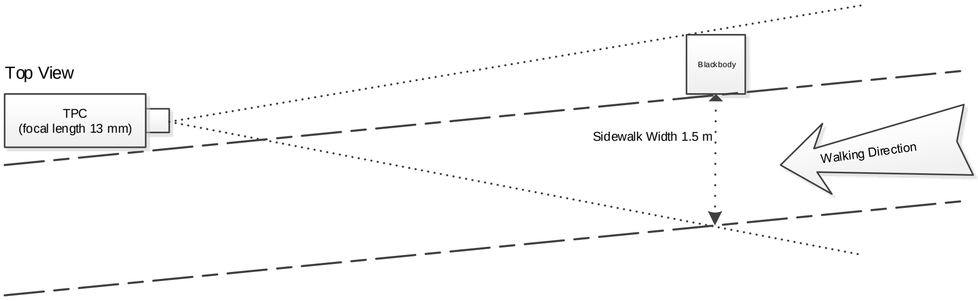


Figure 4-4 Installation (top view)



4.2 Installing Express Service

Server Requirements

Follow this table to prepare a server for installing Express service.

Table 4-2 Server configuration requirement

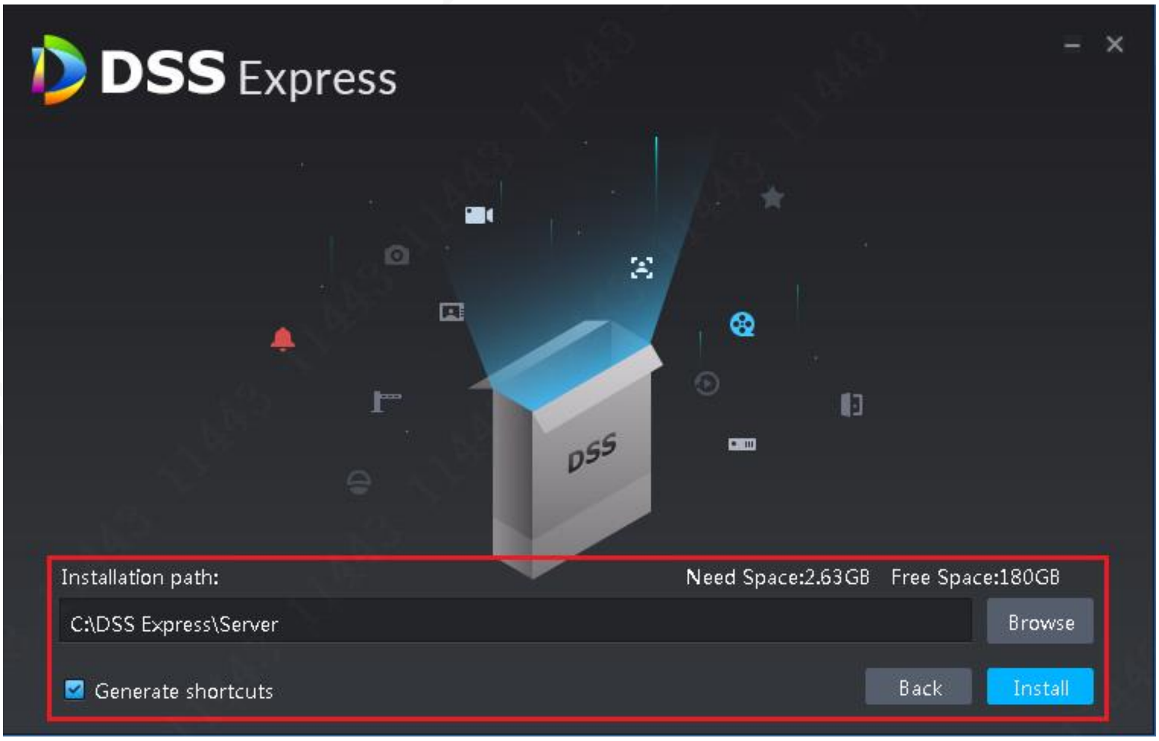
DSS Server Configuration Requirement	
Recommended config	● CPU: Intel® Xeon® CPU E3-1220 v5 @3.00GHz ● RAM: 8 GB ● Network adapter: 1Gps ● DSS installation directory space: Over 500 GB
Minimum config	● CPU: i3-2120 ● RAM: 8 GB ● Network adapter: 1Gps ● DSS installation directory space: Over 200 GB
System	Support Win7 and later systems. 📖 The manual takes Windows Server 2012 R2 as an example to introduce how to configure server IP address and system time.

Installing Program

Step 1 Double-click installer.

Step 2 Select I have read and agree the DSS agreement, and then click Next.

Figure 4-5 Select installation path



Installation path: C:\DSS Express\Server

Need Space:2.63GB Free Space:180GB

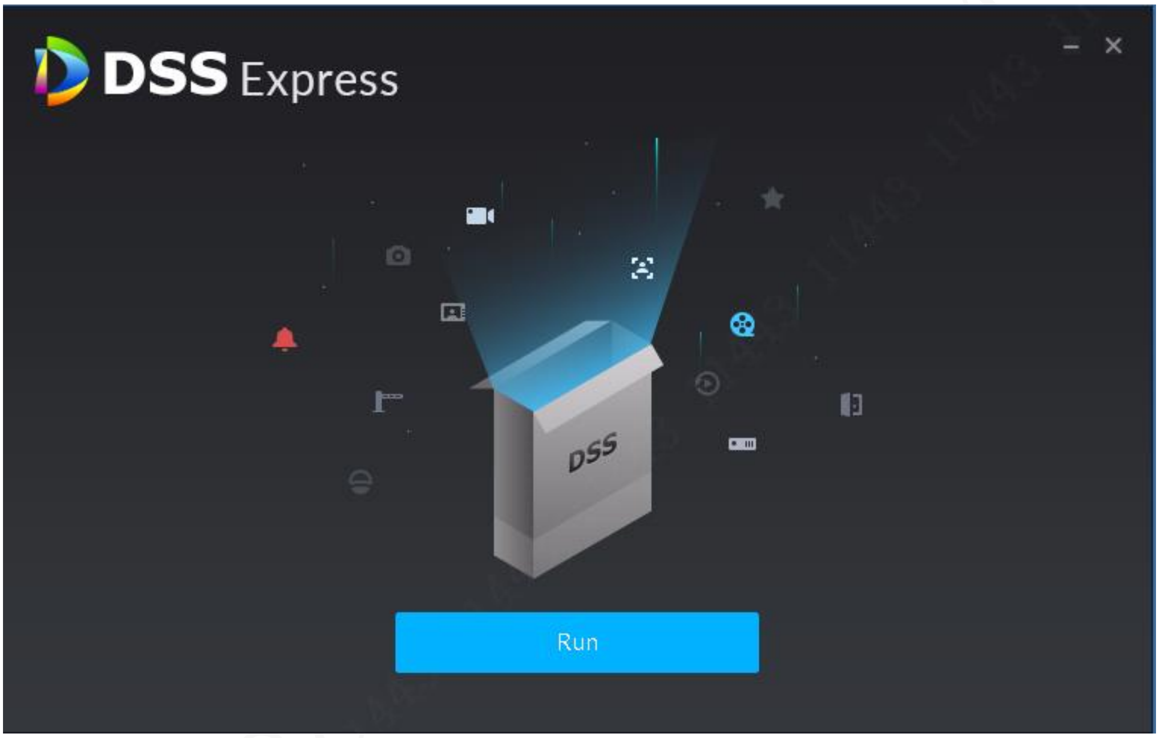
☑ Generate shortcuts

Step 3 Click **Browse** and select installation path, click **Install**.

The system displays installation progress, the whole installation needs 5-10 minutes. See Figure 4-6 after installation is completed. The server starts automatically after installation.

- The system automatically detects the available space of path after the installation path is selected, if available space is less than needed for system installation, then the icon **Install** becomes gray, and installation cannot be implemented.
- Do not select **Generate Shortcuts** if it is not necessary.
- If port conflict exists, the system will prompt conflicted port during installation. Open DSS Express Server and modify port after installation is completed.

Figure 4-6 Installation completed



Step 4 Click **Run**.

The network card selection interface is displayed.

Step 5 Select a network card, and then click **Next**.

The security setting interface is displayed.

Step 6 Enable or disable TLS1.0 protocol as needed.

If TLS1.0 is disabled on Express, to use the platform, you need to enable TLS1.1 and TLS1.2 on the browser.

Step 7 Click **OK**.

4.3 Installing Express PC Client

PC Configuration Requirement

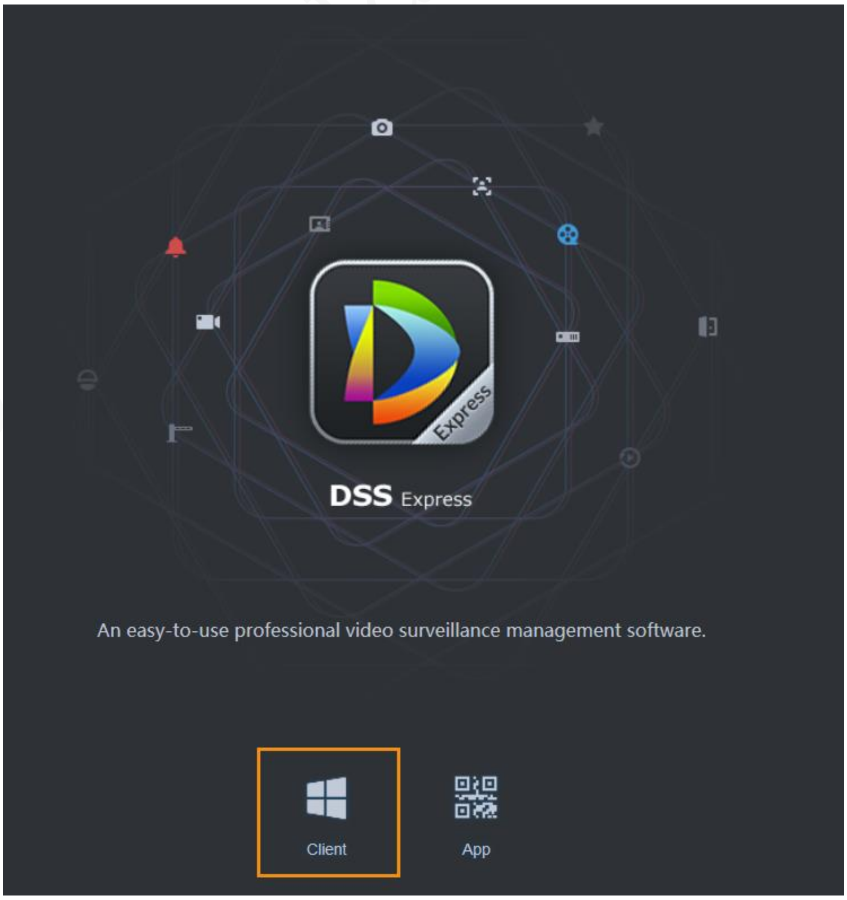
Table 4-3 Configuration requirement

PC Configuration Requirement	
Recommended Config	● CPU: i5-6500 ● Basic frequency: 3.20GHz ● Memory: 8 GB ● Graphic card: Intel® HD Graphics 530 ● Network adapter: 1Gbps ● DSS client installation directory space: 100 GB
Min Config	● CPU: i3-2120 ● Memory: 4 GB ● Graphic card: Intel (R) Sandbridge Desktop Gra ● Network adapter: 1Gbps ● DSS installation directory space: 50 GB

Download and Install

Step 1 Enter server IP address into browser, click **Enter**.

Figure 4-7 Download client



An easy-to-use professional video surveillance management software.

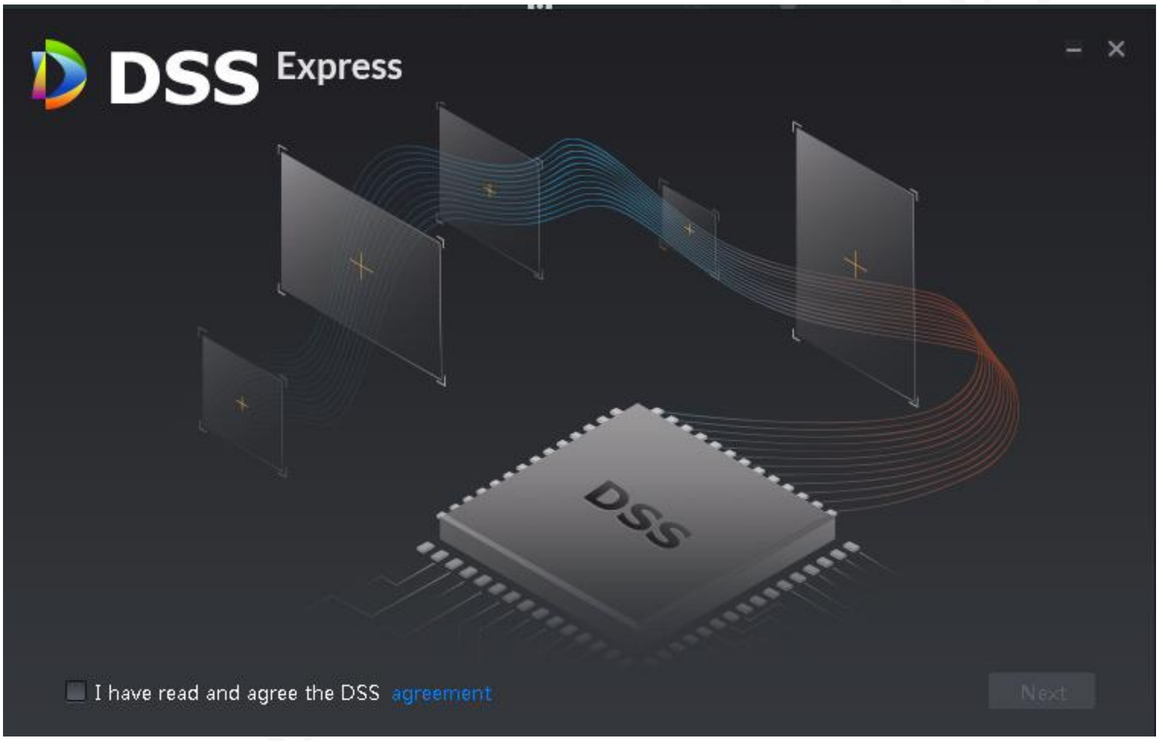
Step 2 Double-click ⊞, run or download client according to interface prompt.

Table 4-4 Download operation

Operation	Description
Run	Download temporary file, you can install after it is checked.
Save	Download installation package to IE default path.
Save as	Download installation package to designated path.
Save and Run	Download installation package to IE default path, and you can install after it is checked.

Step 3 Click **Run**, or Double-click client installation program under the save directory.

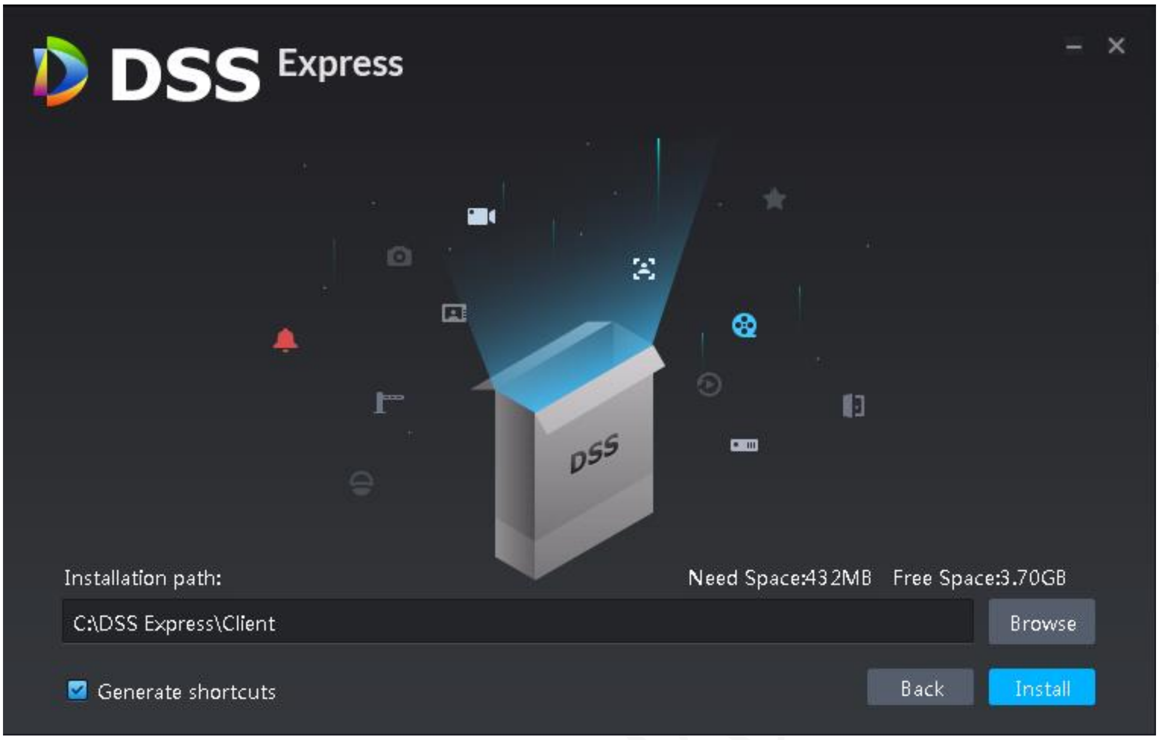
Figure 4-8 Confirm agreement



☐ I have read and agree the DSS agreement

Step 4 Select I have read and agree the DSS agreement, click Next.

Figure 4-9 Select installation path



Installation path:

Need Space:432MB Free Space:3.70GB

C:\DSS Express\Client

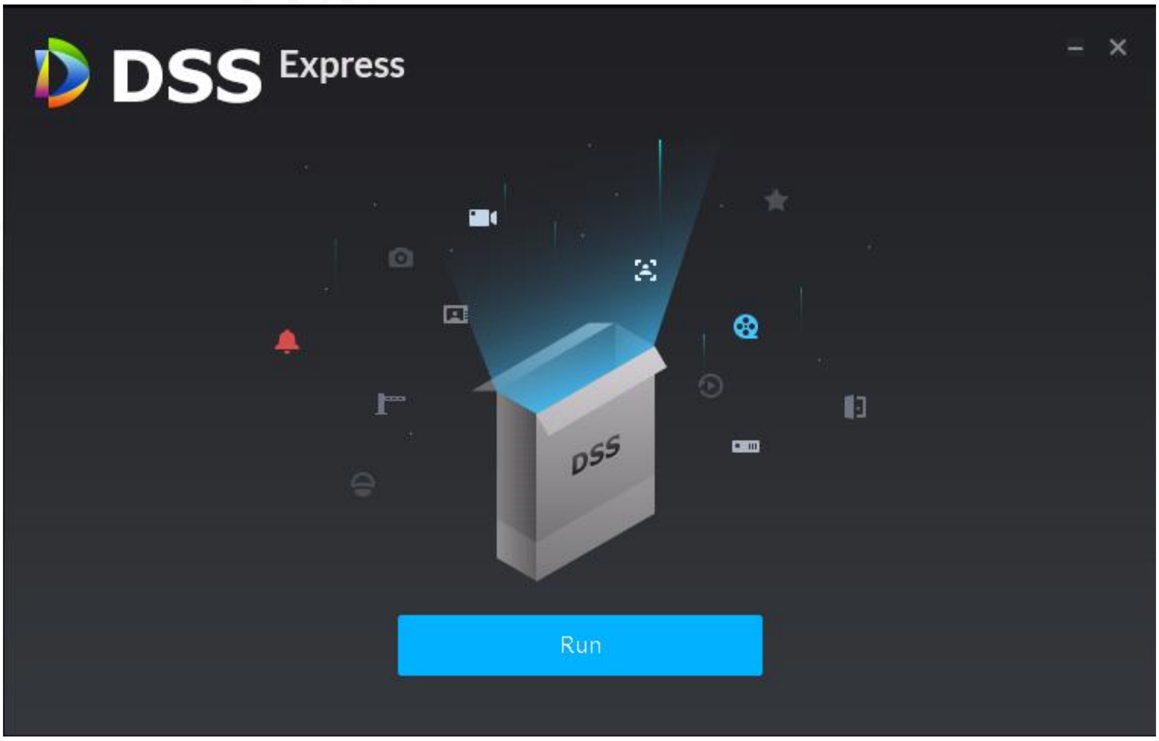
☑ Generate shortcuts

Step 5 Click **Browse** and select installation path, click **Install**.

The system displays installation progress, and the installation takes about 2-3 minutes. The interface is shown after installation is completed.

- The system automatically detects the available space of path after the installation path is selected, if available space is less than needed for system installation, then the icon **Install** becomes gray, and installation cannot be implemented.
- Do not select **Generate Shortcuts** if it is not necessary.

Figure 4-10 Installation completed



4.4 Installing DMSS

Use Google Play to download DMSS and then install it.

5 Getting Started

Based on your product combination and networking method (refer to "2 Network Diagram"), partially follow this chapter to initialize and configure your devices.

5.1 Initializing TPC, IVSS and NVR

5.1.1.1 Initializing TPC, IVSS and NVR

Initialize your TPCs, IVSS and NVRs with ConfigTool for first-time use. To acquire the configuration tool, go to Dahua official website, and then select **Support** > **Download Center** > **ToolBox**, follow the on-screen instructions to download and install the tool.

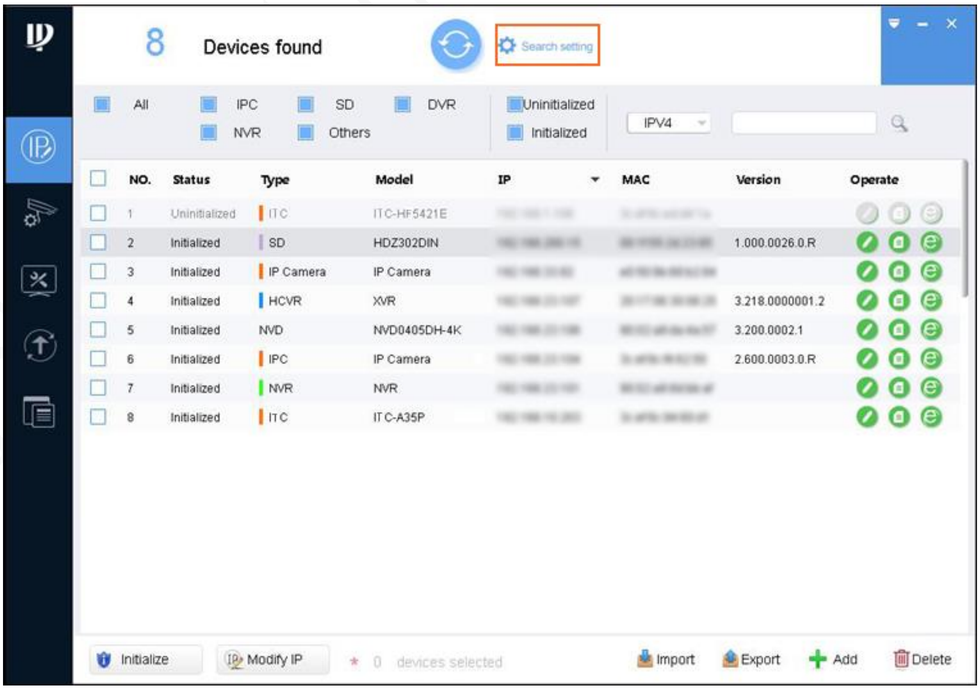
📖

- Device initialization is available only when the IP addresses of the device (192.168.1.108 by default) and the PC stay in the same network segment.
- Plan useable network segment properly to connect the device to the network.
- The following figures and interfaces are for reference only, and the actual product shall prevail.

Step 1 Double-click ConfigTool.exe to open the tool.

Step 2 Click Ⓟ.

Figure 5-1 Modify IP



8 Devices found

Search setting

■ All ■ IPC ■ SD ■ DVR ■ Uninitialized IPV4
■ NVR ■ Others ■ Initialized

□	NO.	Status	Type	Model	IP	MAC	Version	Operate
□	1	Uninitialized	ITC	ITC-HF5421E	[redacted]	[redacted]		
□	2	Initialized	SD	HDZ302DIN	[redacted]	[redacted]	1.000.0026.0.R	
□	3	Initialized	IP Camera	IP Camera	[redacted]	[redacted]		
□	4	Initialized	HCVR	XVR	[redacted]	[redacted]	3.218.0000001.2	
□	5	Initialized	NVD	NVD0405DH-4K	[redacted]	[redacted]	3.200.0002.1	
□	6	Initialized	IPC	IP Camera	[redacted]	[redacted]	2.600.0003.0.R	
□	7	Initialized	NVR	NVR	[redacted]	[redacted]		
□	8	Initialized	ITC	ITC-A35P	[redacted]	[redacted]		

Step 3 Click Search Setting.

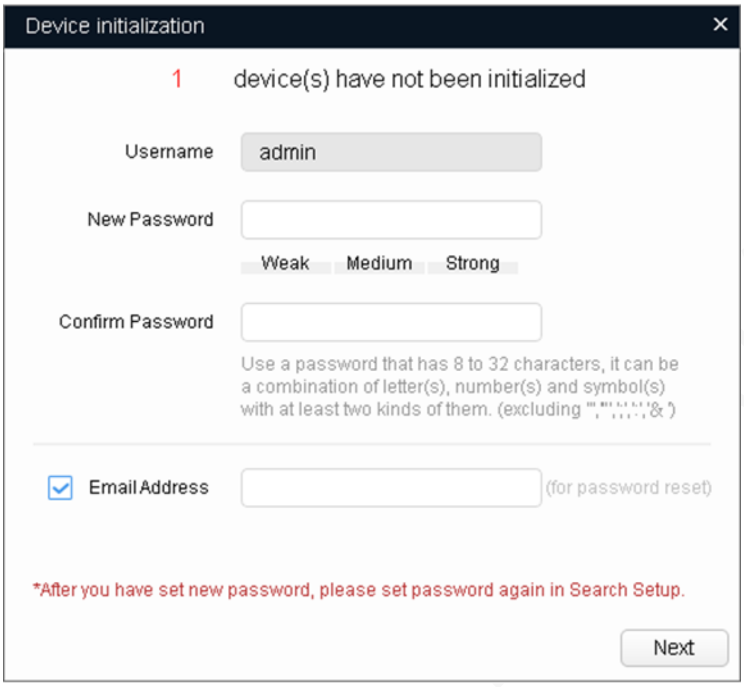
Step 4 Enter the start IP address and end IP address of the network segment in which you want to search for devices, and then click **OK**.

All the devices found in the network segment are listed.

Step 5 Select one or several devices with **Status** shows **Uninitialized**, and then click **Initialize**.

Step 6 Select the devices that need initialization, and then click **Initialize**.

Figure 5-2 Password setting



Device initialization

1 device(s) have not been initialized

Username: admin

New Password:

Weak Medium Strong

Confirm Password:

Use a password that has 8 to 32 characters, it can be a combination of letter(s), number(s) and symbol(s) with at least two kinds of them. (excluding "'",""",";",":",'&')

☑ Email Address: (for password reset)

*After you have set new password, please set password again in Search Setup.

Step 7 Set and confirm the password of the devices, then enter a valid email address, and then click **Next**.

Password can be modified or reset in **System Settings**.

Step 8 Select the options according to your needs, and then click **OK**.

Click the success icon (✓) or the failure icon (⚠) for the details.

Step 9 Click **Finish**.

The device status in the **Modify IP** interface turns to **Initialized**.

5.1.1.2 Modifying Device IP Address

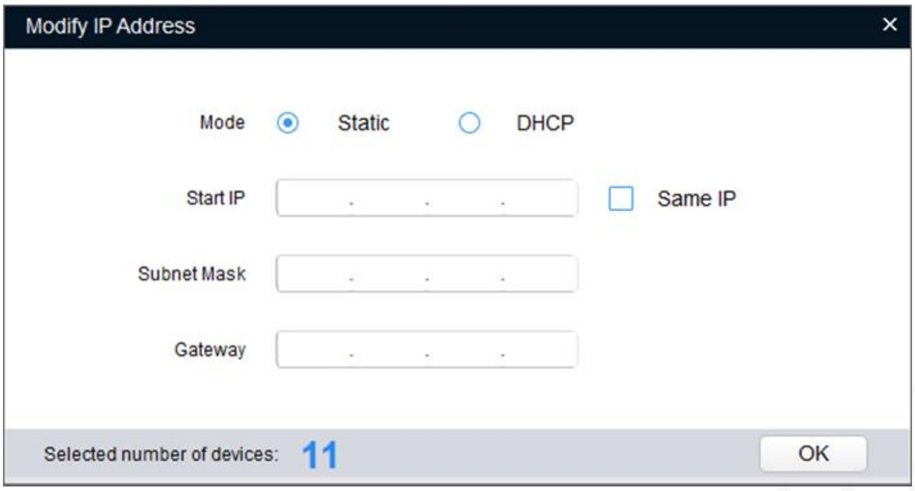
- You can modify IP address of one or multiple devices in one time. This section is based on modifying IP addresses in batches.
- Modifying IP addresses in batches is available only when the corresponding devices have the same login username and password.

Step 1 Do "Step 1" to "Step 4" in "5.1.1.1 Initializing TPC, IVSS and NVR" to search for devices in your network segment.

After clicking **Search setting**, enter the username and password, and please make sure that that they are the same as what you set during initialization, otherwise there will be "wrong password" notice.

Step 2 Select the devices which IP addresses need to be modified, and then click **Modify IP**.

Figure 5-3 Modify IP Address



Modify IP Address ×

Mode ● Static ○ DHCP

Start IP . . . □ Same IP

Subnet Mask . . .

Gateway . . .

Selected number of devices: 11

OK

Step 3 Select **Static** mode, and then enter start IP, subnet mask, and gateway. All the IP addresses will be modified sequentially from the start IP.

If DHCP server is available in the network, devices will automatically obtain IP addresses from DHCP server when you select **DHCP**.

Step 4 Click **OK**.

5.1.1.3 Updating System

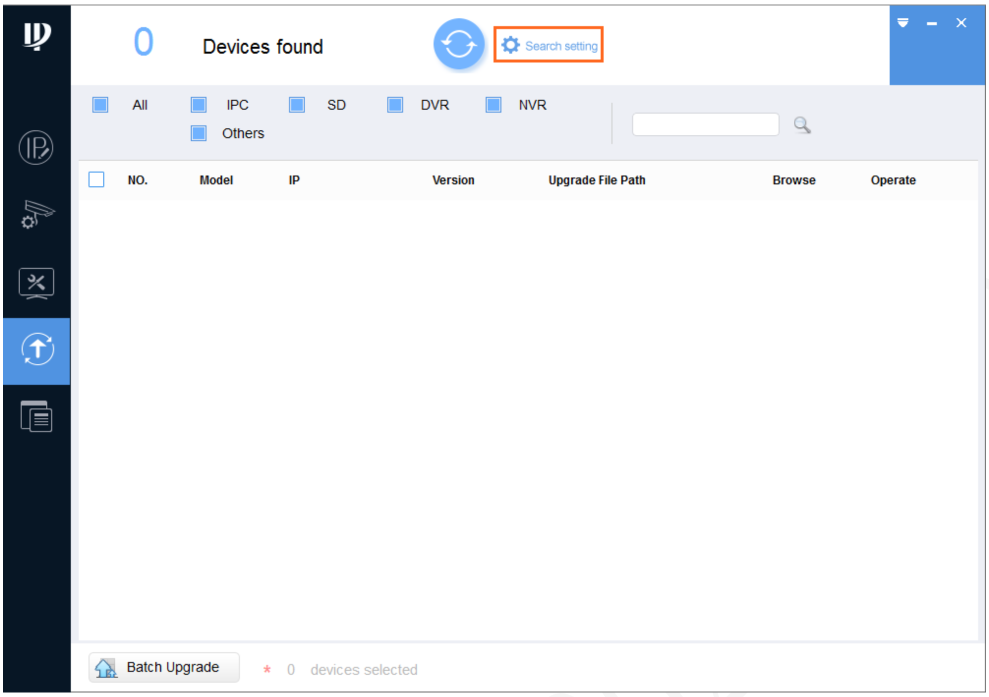
ConfigTool supports updating devices one by one or in batches.

- Updating devices one by one is ideal when few devices are involved, and login username and password of the devices are different.
- Updating devices in batches is recommended when multiple devices are involved, and login username and passwords of cameras are the same.

Step 1 Double-click "ConfigTool.exe" to open the tool.

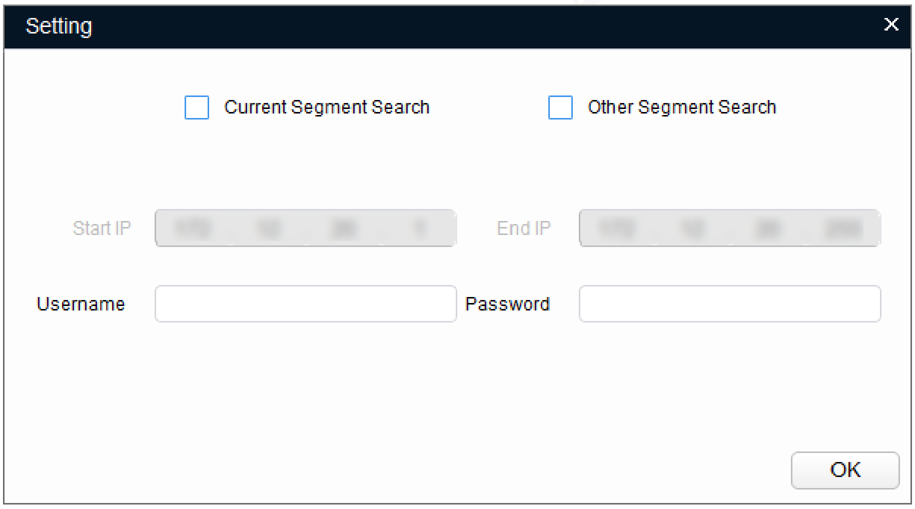
Step 2 Click ⬆.

Figure 5-4 Update



Step 3 Click Search setting.

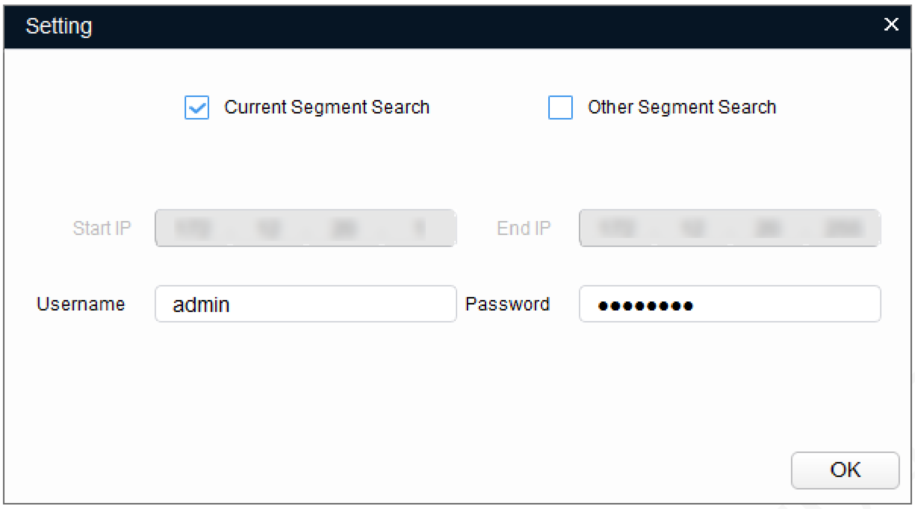
Figure 5-5 Search setting



Step 4 Select the network segment for the target device.

- If the IP address of the target device is in the current network segment, select **Current Segment Search**, and then enter the user name and the password of the target camera.

Figure 5-6 Current segment search



Setting

☑ Current Segment Search □ Other Segment Search

Start IP

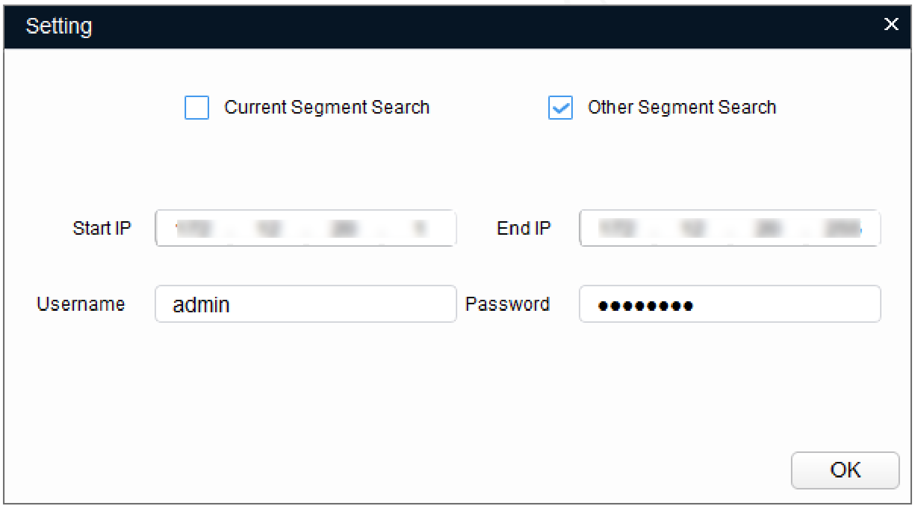
End IP

Username: admin

Password: ••••••••

- If the IP address of the target device is in other network segment, select **Other Segment Search**, then enter the start IP address and end IP address of the network segment you need, and then enter the user name and the password of the target camera.

Figure 5-7 Other segment search



Setting

□ Current Segment Search ☑ Other Segment Search

Start IP

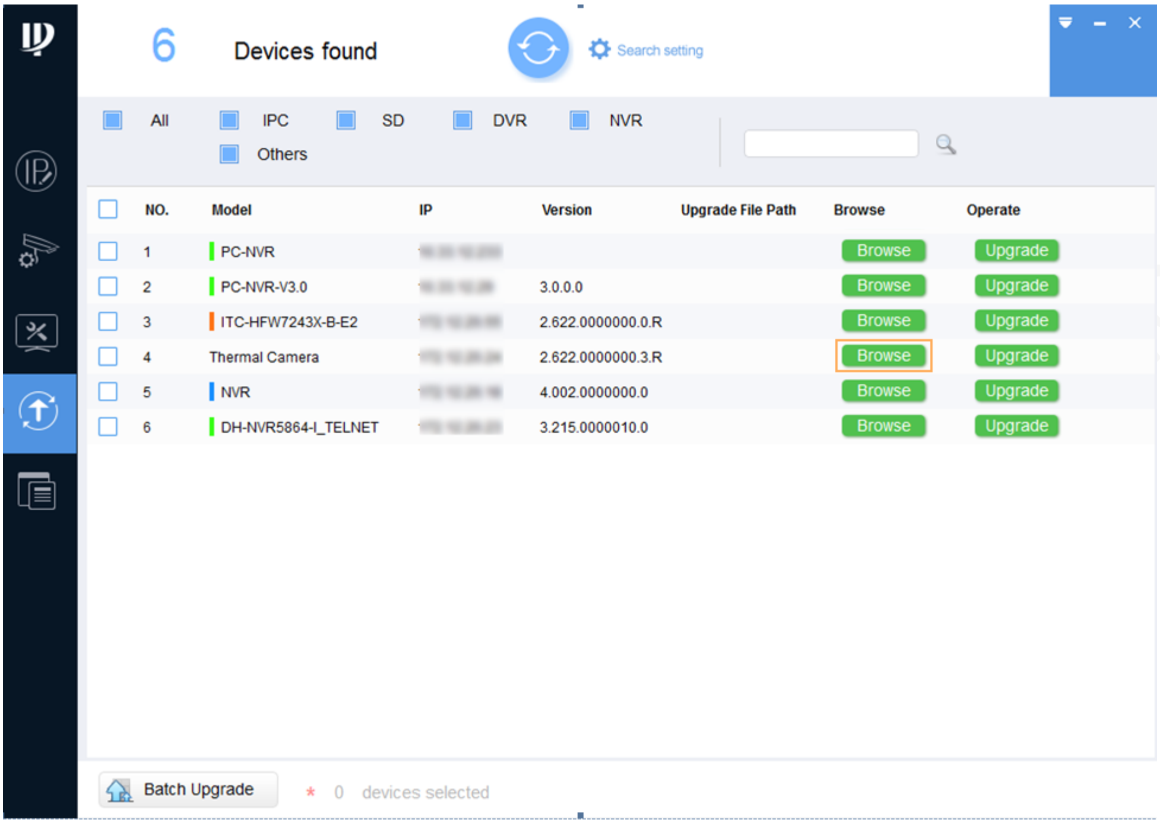
End IP

Username: admin

Password: ••••••••

Step 5 Click **OK**.

Figure 5-8 Search result



6 Devices found

☑ All ☑ IPC ☑ SD ☑ DVR ☑ NVR ☑ Others

□	NO.	Model	IP	Version	Upgrade File Path	Browse	Operate
□	1	PC-NVR	[redacted]			Browse	Upgrade
□	2	PC-NVR-V3.0	[redacted]	3.0.0.0		Browse	Upgrade
□	3	ITC-HFW7243X-B-E2	[redacted]	2.622.0000000.0.R		Browse	Upgrade
□	4	Thermal Camera	[redacted]	2.622.0000000.3.R		Browse	Upgrade
□	5	NVR	[redacted]	4.002.0000000.0		Browse	Upgrade
□	6	DH-NVR5864-I_TELNET	[redacted]	3.215.0000010.0		Browse	Upgrade

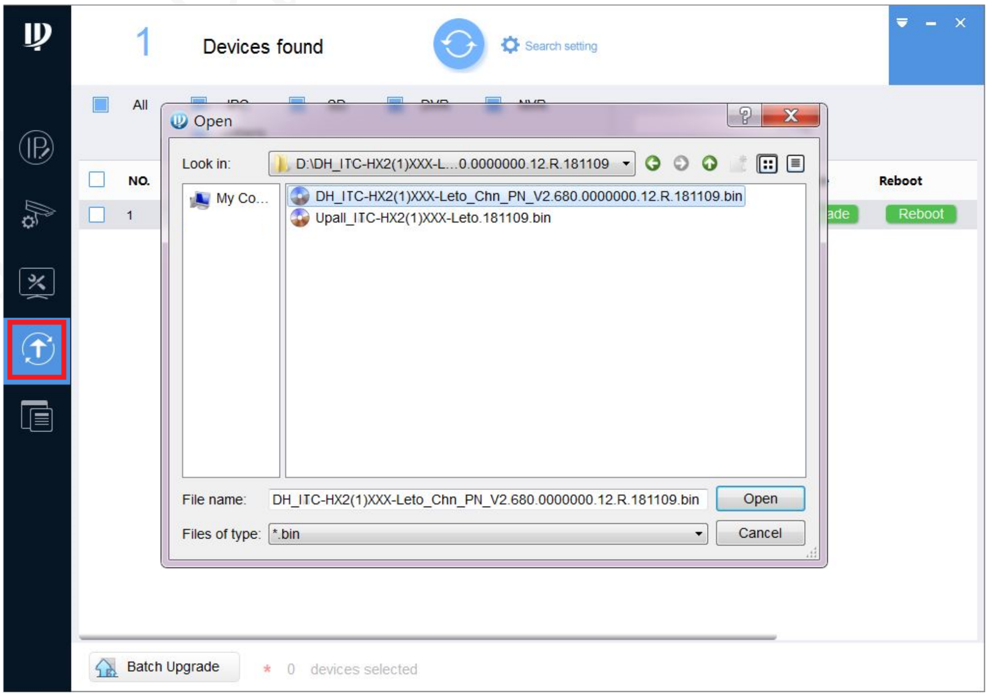
Batch Upgrade * 0 devices selected

Step 6 Select the devices to update.

- Update devices one by one: Select the corresponding device, and then click **Browse**.
- Update devices in batches: Select multiple devices, and then click **Batch Upgrade**.

Step 7 Select the update file.

Figure 5-9 Browse



1 Devices found

Open

Look in: D:\DH_ITC-HX2(1)XXX-L…0.0000000.12.R.181109

My Co…

DH_ITC-HX2(1)XXX-Leto_Chn_PN_V2.680.0000000.12.R.181109.bin

Upall_ITC-HX2(1)XXX-Leto.181109.bin

File name: DH_ITC-HX2(1)XXX-Leto_Chn_PN_V2.680.0000000.12.R.181109.bin

Files of type: *.bin

Open

Cancel

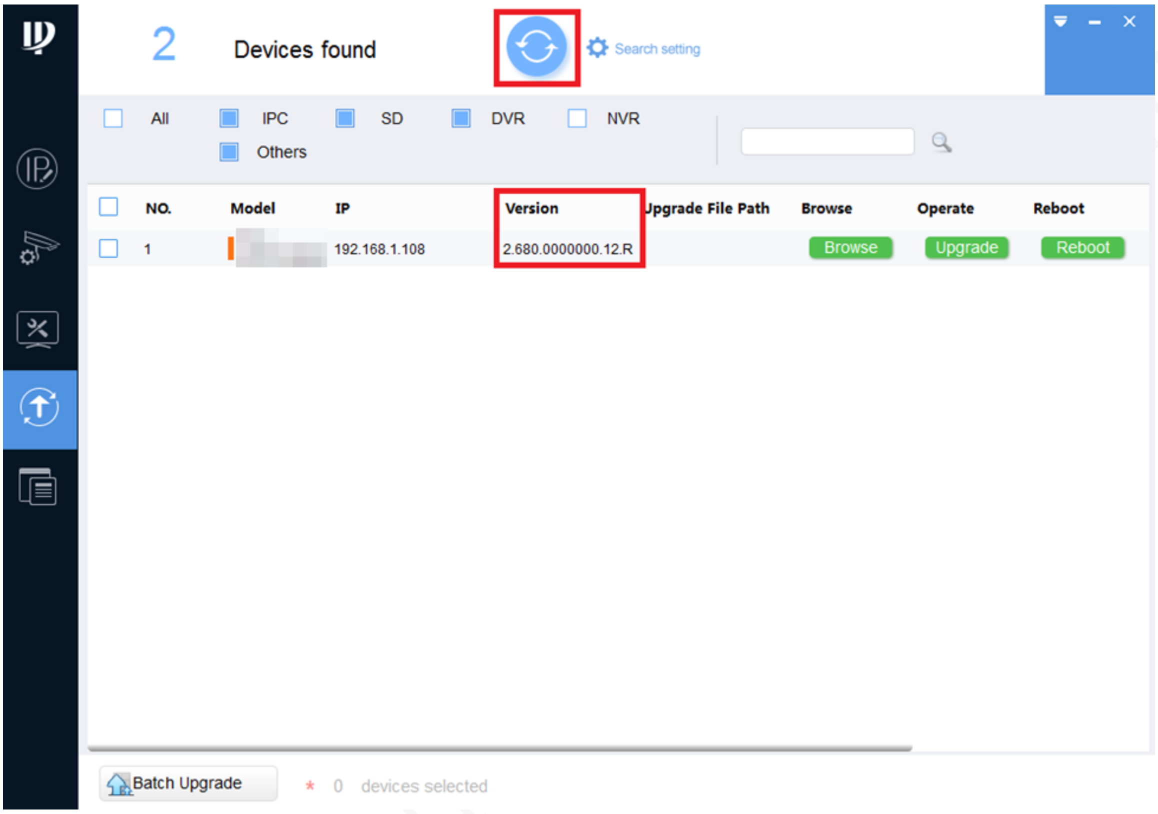
Batch Upgrade * 0 devices selected

Step 8 Update the devices.

- Update the devices one by one: Click **Upgrade**, and the system starts updating. You can see the update progress.
- Update the devices in batches: Click **OK**, and the system starts updating.

Step 9 After restarting the device, click the refresh button to confirm the system version.

Figure 5-10 Confirm version



□	NO.	Model	IP	Version	Jpgrade File Path	Browse	Operate	Reboot
□	1	[redacted]	192.168.1.108	2.680.0000000.12.R		Browse	Upgrade	Reboot

The update succeeded if the **Version** is the same as the version of the update file.

⚠

If the update failed, you can:

- Check whether the update file is correct.
- Restart the ConfigTool and do the update again.

5.2 Initializing and Logging in to Express

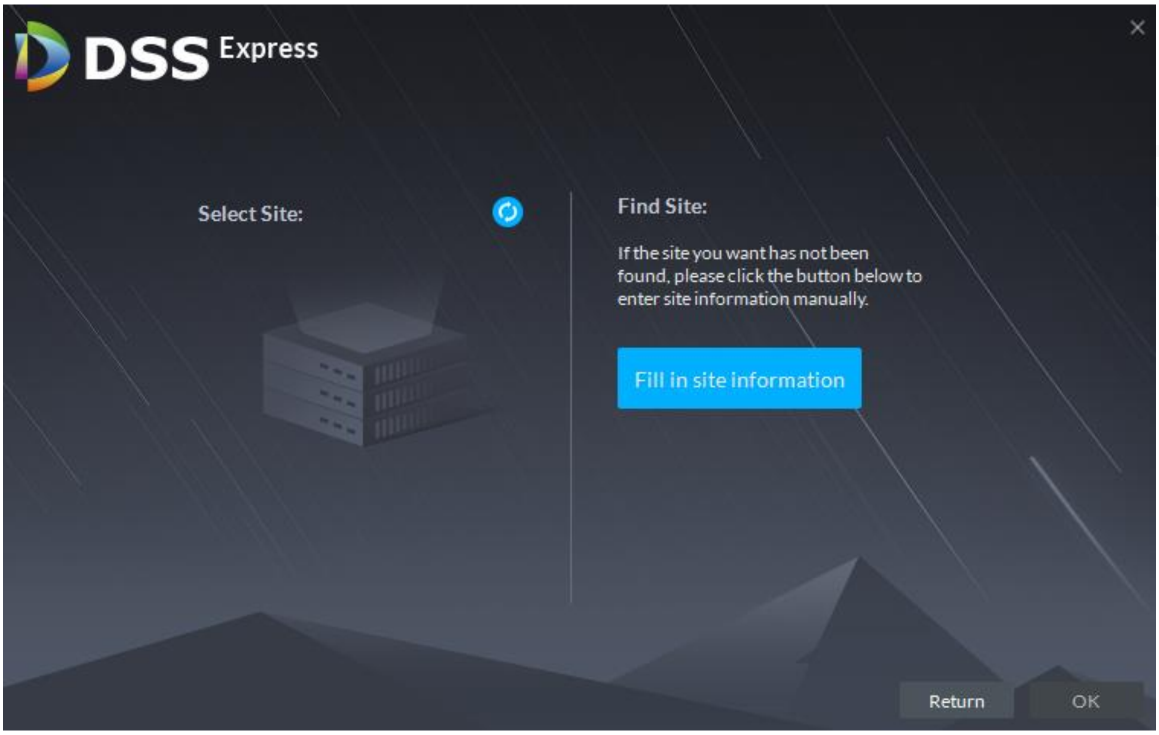
Install and activate your Express before you can use it normally. Skip this chapter if you do not use Express.

5.2.1.1 Initialization Configurations

You need to initialize server if you log in for the first time. Modify password, set security questions for system user. You can find password by answering questions when you forget password.

Step 1 Double-click DSS Express Client on server desktop, or click **Run** on the interface after program is installed.

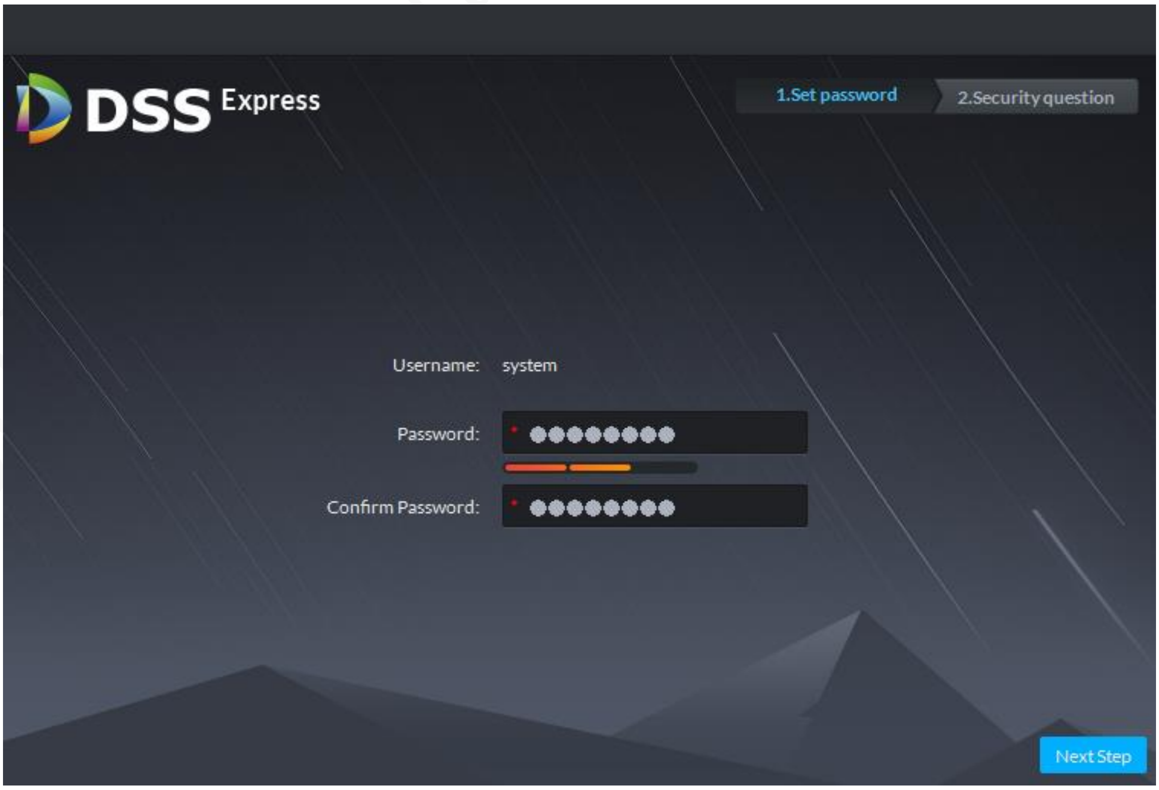
Figure 5-11 Log in to control client (1)


DSS Express
Select Site:
Find Site:
If the site you want has not been found, please click the button below to enter site information manually.
Fill in site information
Return
OK

Step 2 Select a detected server on the left of the interface, or click **Fill in site information**, enter in IP address and port number.

Step 3 Click **OK**.

Figure 5-12 Set password



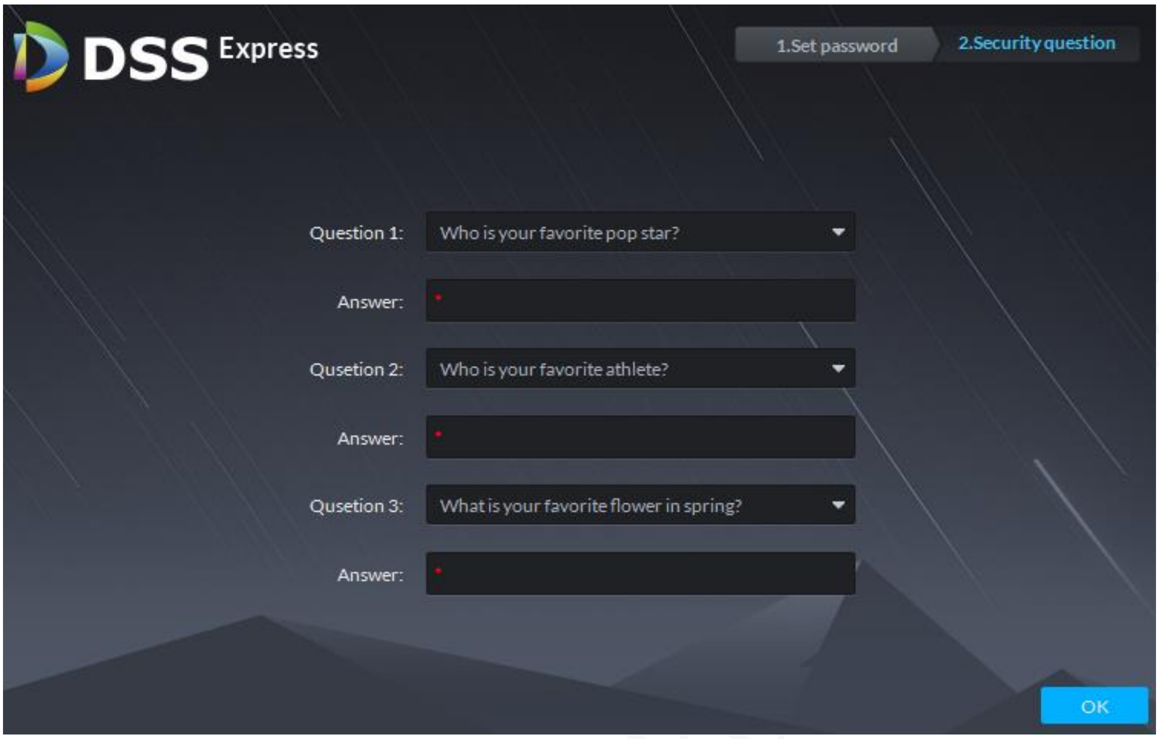
Username: system

Password: ●●●●●●●●

Confirm Password: ●●●●●●●●

Step 4 Enter new password, and then click **Next**.

Figure 5-13 Security question



DSS Express

1.Set password
2.Security question

Question 1: Who is your favorite pop star?

Answer: *

Qusetion 2: Who is your favorite athlete?

Answer: *

Qusetion 3: What is your favorite flower in spring?

Answer: *

Step 5 Select questions, set answers, and then click **OK**.

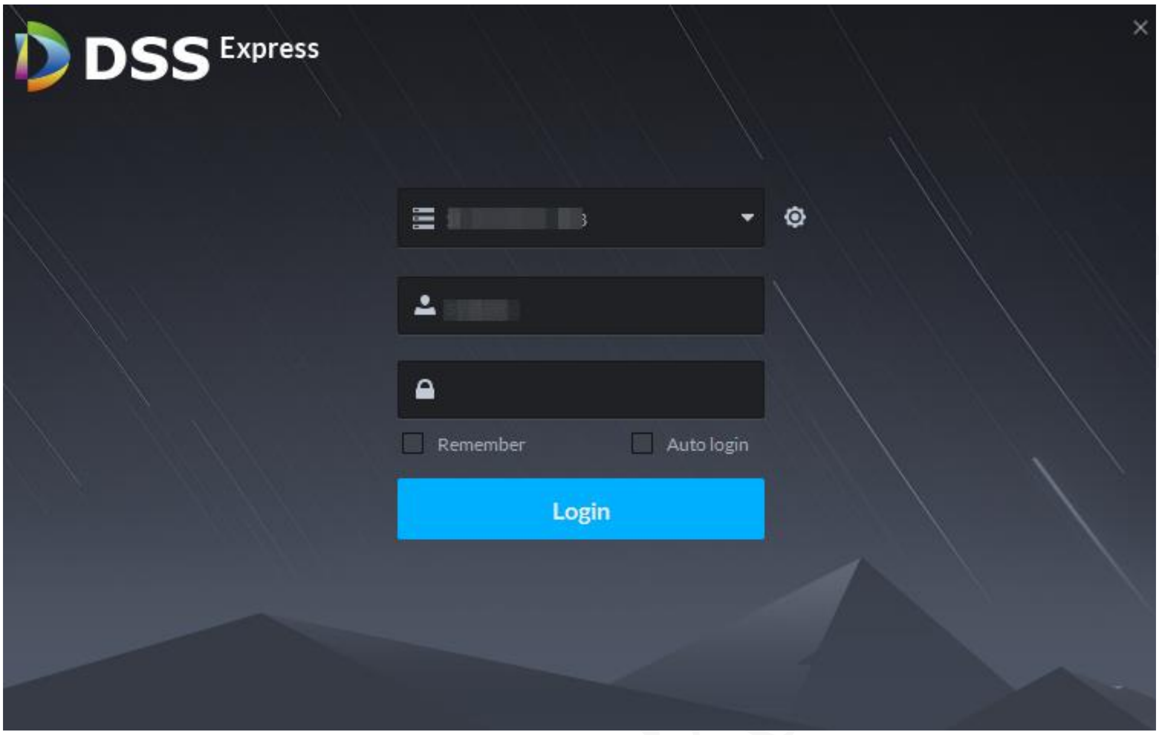
The **Homepage** interface is displayed.

5.2.1.2 Logging in to Express

You can configure and manage the system remotely by using the client.

Step 1 Double-click the shortcut icon DSS Express Client on the server desktop, or click **Run** on the program interface after the program installation is completed.

Figure 5-14 Client login interface



Step 2 Select the detected server, enter username and password, and then click **Login**.

5.2.1.3 Licensing Express

Make sure that you have purchased a proper license for activating Express. To purchase a license, contact our local sales team.

This section introduces how to import your license file to activate Express.

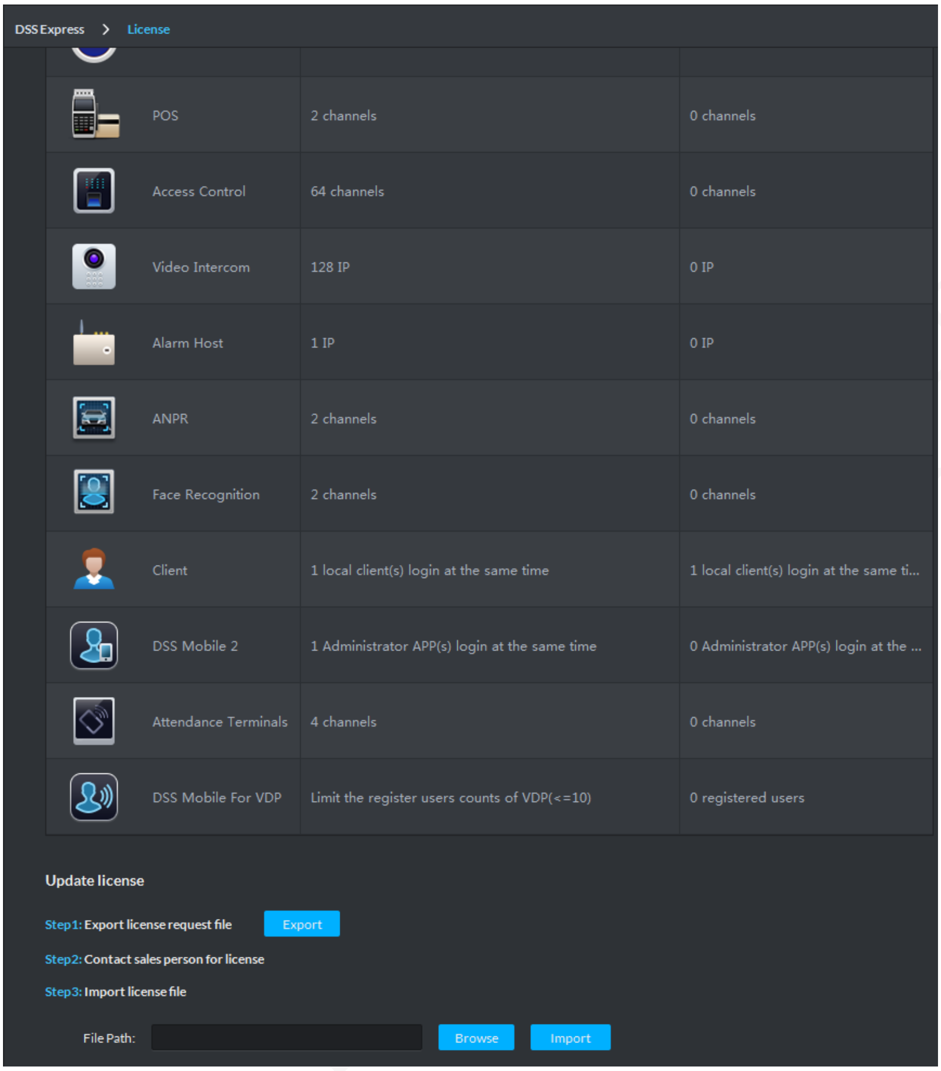
Step 1 Log in to Express client.

Step 2 On the client homepage, select **Config > License**.

Step 3 Click Update License.

The system moves to the license update section.

Figure 5-15 Update license



DSS Express > License

POS	2 channels	0 channels
Access Control	64 channels	0 channels
Video Intercom	128 IP	0 IP
Alarm Host	1 IP	0 IP
ANPR	2 channels	0 channels
Face Recognition	2 channels	0 channels
Client	1 local client(s) login at the same time	1 local client(s) login at the same ti...
DSS Mobile 2	1 Administrator APP(s) login at the same time	0 Administrator APP(s) login at the ...
Attendance Terminals	4 channels	0 channels
DSS Mobile For VDP	Limit the register users counts of VDP(<=10)	0 registered users

Update license

Step1: Export license request file Export

Step2: Contact sales person for license

Step3: Import license file

File Path: Browse Import

Step 4 Click **Browse**, select License file you want to upload according to system prompt.

Step 5 Click **Import**.

System loads License, after that the system prompts license info is changed and the program restarts.

Step 6 Log in client again, enter license configuration interface, and make sure the License is the same as applied.

5.3 Logging in to DMSS

Step 1 Search for DMSS in Google Play, download, and then install the App.

Step 2 On your mobile phone, tap .

Step 3 Select your region, and then tap **Done**.

You can change your region in **Me > Change Region**.

Step 4 Read User Service Agreement and Privacy Policy.

Step 5 Tap **Sign up**, enter email address and password, select *I have read and agree to* check box, and then tap **Get verification code**.

Step 6 Enter verification code and then tap **Log in**.

Step 7 Tap **Home**.

Figure 5-16 Home

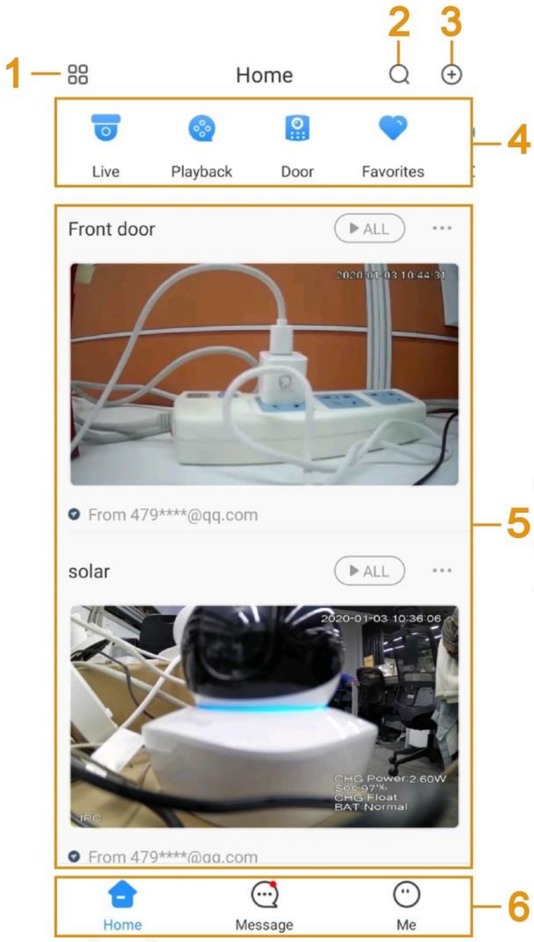


Table 5-1 Home interface descriptions

No.	Function	Description
1	Display mode	Tap ⊞ to switch between displaying devices in list mode or picture mode.
2	Search	Tap 🔍 to search devices or channels with keywords.
3	Add devices	Tap ⊕ to add devices.
4	Function modules	Display the main function modules. Tap and drag the icon to change its place.
5	Devices	Display the added devices. ● Tap a thumbnail under the device name to play a single channel. If a device has several channels, slide thumbnails to the left to view more. ● Tap ▶ALL to play all channels under this device. ● Tap ··· to view device details and top the device or move down.

6	Navigation bar	Three tabs: **Home**, **Message**, and **Me**.

6 Configuration and Commissioning

Configure the alarms on the devices, then video/image storage on IVSS/NVR, and then alarm receiving and viewing on Express/DMSS. This manual is for all the product combinations and if you do not have the product, skip it. (For example, if your product combination is TPC–IVSS–Express, skip NVR and DMSS related contents)

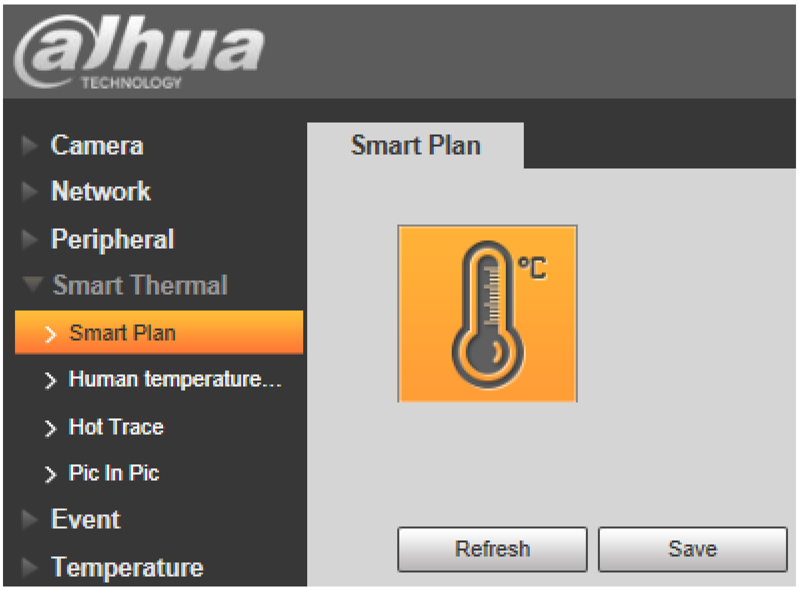
6.1 Configuring TPC

Configure TPC temperature alarm—siren and light to get inspectors notified. Still, elevated body temperature detected by the TPC will be delivered to Face Recognition Terminal, then to Express or DMSS.

6.1.1 Enabling Body Temperature Monitoring Scheme

To use body temperature monitoring scheme, select **Setting > Smart Thermal > Smart Plan** and click 🌡 (the scheme on/off switch) to lighten it. 🌡 represents that the scheme is enabled.

Figure 6-1 Enabling body temperature monitoring scheme



6.1.2 Configuring Body Temperature Alarm

Configure a maximum normal human body temperature. When body temperature is larger than the set value, linked audio and white light alarm will be triggered.

Step 1 On thermal web, select Setting > Smart Thermal > Human Temperature Measurement.

Step 2 Draw a detection area to detect people you need. The detection area requires its lower border near people shoulders (Its upper border can be the image upper edge). Confirm detection area first and then click **Draw Rule** to draw the area.

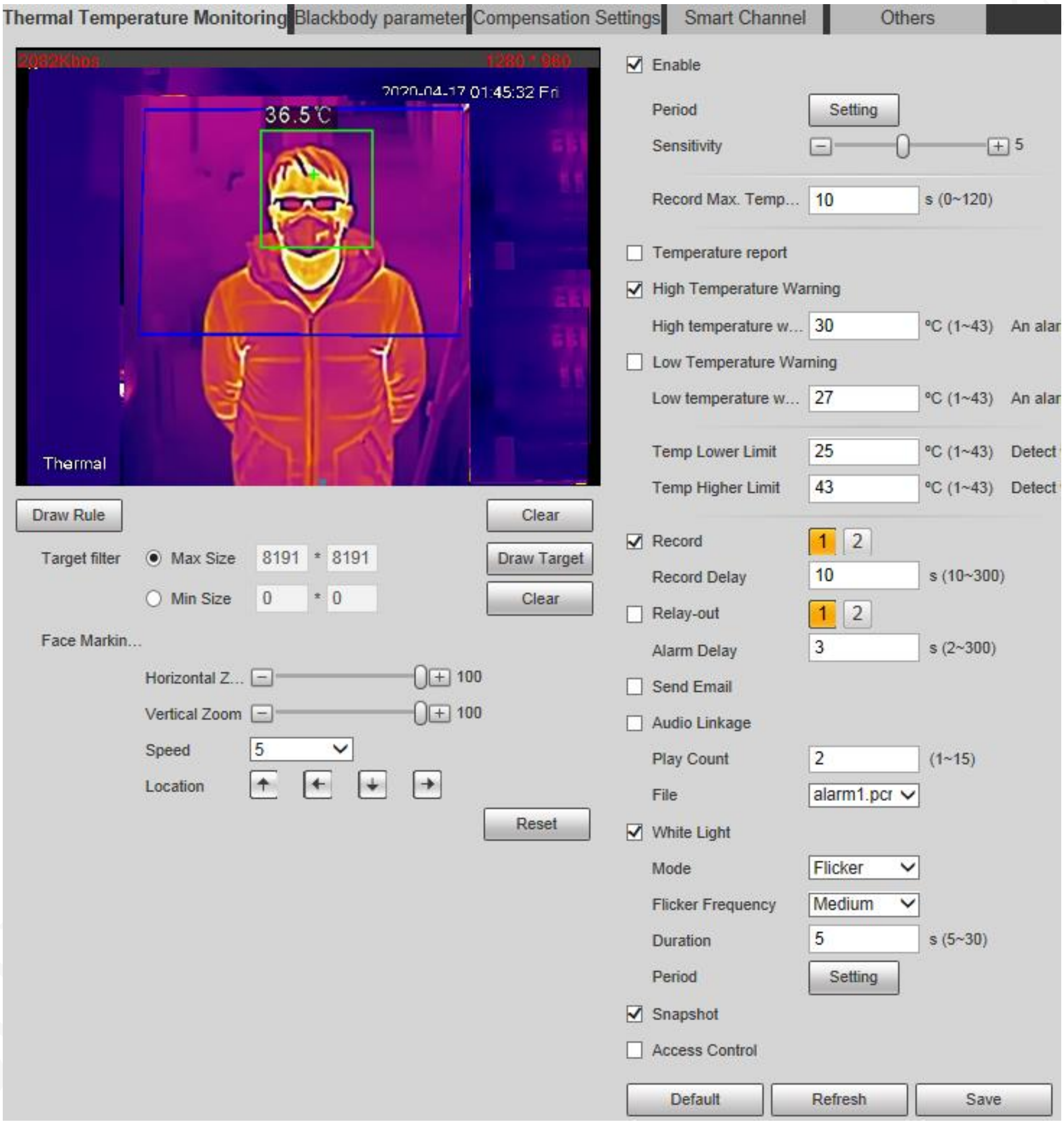
Step 3 Select High temperature abnormal alarm and enter a value.

Step 4 To enable audio alarm, select **Audio Linkage**. To set audio alarm lasting time, enter **Play Count** value.

Step 5 (White light alarm can be used at night or at dark condition). Select **White Light** to enable.

1) To set alarm period (only at night, for example), click **Setting**.
2) To decide white light lasting time, enter **Duration**.
3) To decide white light showing method (flicker or normally on), click **Mode**. If you select **flicker**, you can decide its frequency from **High**, **Medium** and **Low**.

Figure 6-2 Configuring temperature alarm



Thermal Temperature Monitoring | Blackbody parameter | Compensation Settings | Smart Channel | Others

Draw Rule
Clear
Target filter ● Max Size 8191 * 8191
Draw Target
○ Min Size 0 * 0
Clear
Face Markin...
Horizontal Z... 100
Vertical Zoom 100
Speed 5
Location
Reset

☑ Enable
Period Setting
Sensitivity 5
Record Max. Temp... 10 s (0~120)
□ Temperature report
☑ High Temperature Warning
High temperature w... 30 °C (1~43) An alar
□ Low Temperature Warning
Low temperature w... 27 °C (1~43) An alar
Temp Lower Limit 25 °C (1~43) Detect
Temp Higher Limit 43 °C (1~43) Detect
☑ Record 1 2
Record Delay 10 s (10~300)
□ Relay-out 1 2
Alarm Delay 3 s (2~300)
□ Send Email
□ Audio Linkage
Play Count 2 (1~15)
File alarm1.pcr
☑ White Light
Mode Flicker
Flicker Frequency Medium
Duration 5 s (5~30)
Period Setting
☑ Snapshot
□ Access Control
Default Refresh Save

Step 6 Click **Save**.

6.1.3 Configuring Blackbody Parameters

Step 1 On the blackbody rear panel, set blackbody temperature to 35 °C (recommended). Press the bottom '︿' '﹀' to adjust the blackbody temperature value.

Step 2 Follow "4 Installation and Connection" to install blackbody.

Step 3 Go to TPC web, select Setting > Smart Thermal > Human Temperature Measurement > Blackbody Parameter.

Make sure blackbody is put at the top left or top right of thermal image.

Step 4 Select **Enable** to enable the parameters configured on this interface.

Step 5 Click **Draw Area** and then draw a box around the blackbody. The smaller the selection box, the higher the measurement accuracy.

Then TPC can recognize blackbody temperature as a reference to help detect human body temperature.

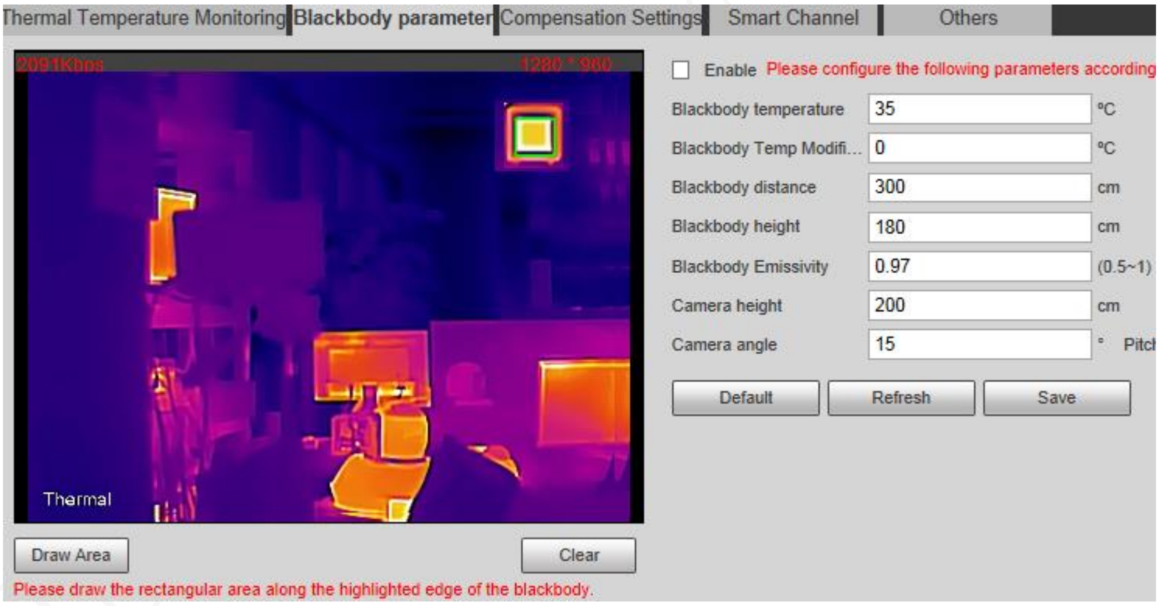
Step 6 Configure other parameters.

- Blackbody temperature: 35°C recommended.
- Blackbody height and camera height: For general scenario, 180 cm for blackbody and 200 cm for TPC.

For scenarios such as junior school, students might generally be shorter than 180 cm, so in this case you need to adjust blackbody height first and then TPC height. For details, consult technical support.

- Others: Leave them to default.

Figure 6-3 Setting blackbody parameters



□ Enable Please configure the following parameters according

Blackbody temperature	35	°C
Blackbody Temp Modifi...	0	°C
Blackbody distance	300	cm
Blackbody height	180	cm
Blackbody Emissivity	0.97	(0.5~1)
Camera height	200	cm
Camera angle	15	° Pitcl

Please draw the rectangular area along the highlighted edge of the blackbody.

Step 7 Click **Save**.

6.1.4 Configuring Temperature Correction

TPC uses blackbody to help monitor body temperature. Still, there might be various factors to influence monitoring accuracy such as environment temperature. So, after you have configured "6.1.1–6.1.3", you still need to verify and calibrate monitoring accuracy.

Step 1 Calibrate measurement accuracy.

1) Choose a group of people (5, for example) and use TPC to monitor their temperature. Write down and calculate their temperature average value (A).

2) Use high monitoring accuracy devices (a point thermometer, for example) to monitor the group temperature and calculate its average value (B).

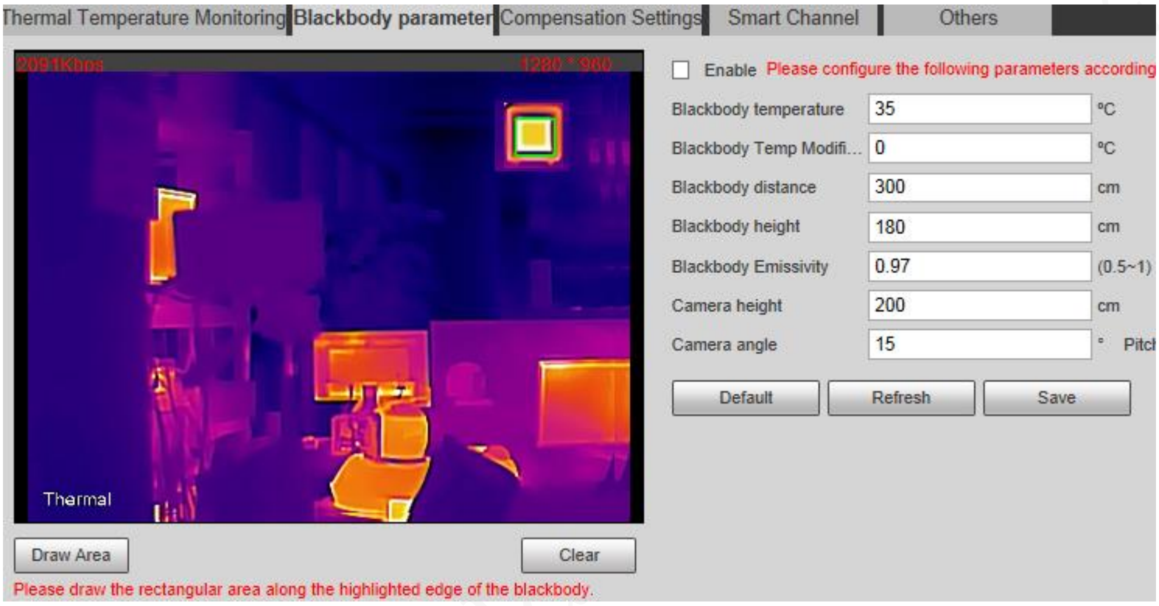
3) Use A to minus B to get the error value (C).

◇ If C is 0, it proves no temperature error and you can ignore Step 2.

◇ If C is not 0, go to Step 2.

Step 2 On TPC web, select **Setting > Smart Thermal > Human Temperature Measurement > Blackbody Parameter** and then enter C in the Blackbody Temperature Correction box. Then click **Save**.

Figure 6-4 Setting alarm temperature correction



☐ Enable Please configure the following parameters according

Blackbody temperature 35 °C

Blackbody Temp Modifi... 0 °C

Blackbody distance 300 cm

Blackbody height 180 cm

Blackbody Emissivity 0.97 (0.5~1)

Camera height 200 cm

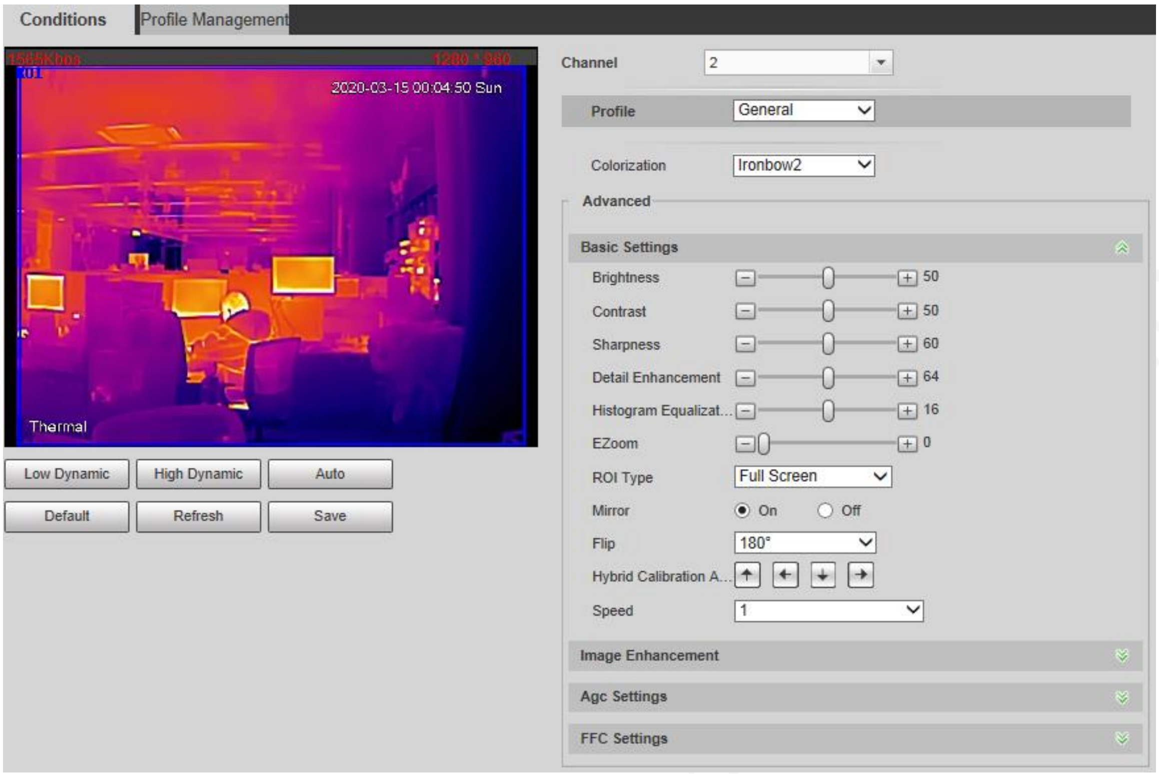
Camera angle 15 ° Pitcl

Please draw the rectangular area along the highlighted edge of the blackbody.

6.1.5 Adjusting Face Detection Box

Within body temperature detection box you have drawn, TPC face detection box might not fit face well. You can select **Setting > Camera > Conditions > Conditions** and adjust up, down, left and right arrows (and set step length) to make the face detection box accurate.

Figure 6-5 Adjusting TPC face box (1)



Channel: 2

Profile: General

Colorization: Ironbow2

Brightness: 50

Contrast: 50

Sharpness: 60

Detail Enhancement: 64

Histogram Equalizat...: 16

EZoom: 0

ROI Type: Full Screen

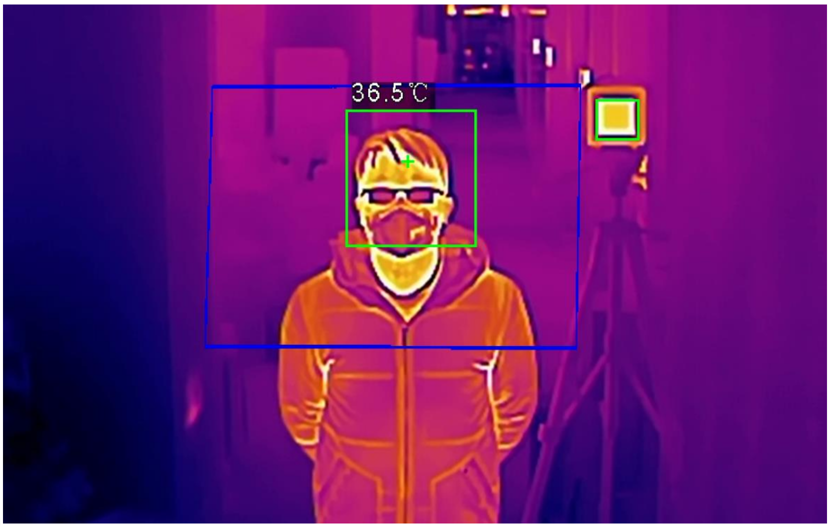
Mirror: ● On ○ Off

Flip: 180°

Hybrid Calibration A...

Speed: 1

Figure 6-6 Adjusting TPC face detection box (2)



The green box around face is face detection box and the larger blue box around body is body temperature detection area.

6.2 Configuring IVSS

Skip this chapter if you do not have IVSS in your product combination.

6.2.1 Adding TPC to IVSS

IVSS supports smart add, manual add and template add.

Table 6-1 Mode of adding TPC

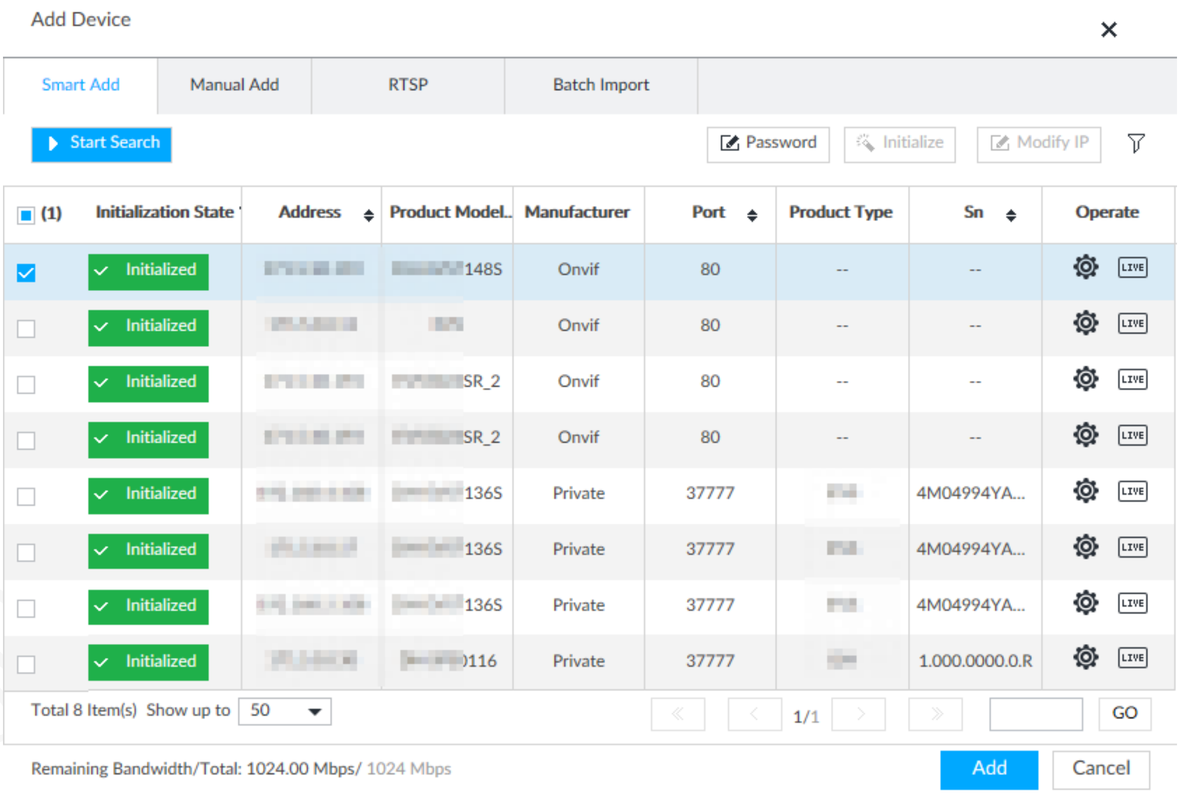
Mode	Description
Smart Add	Search the remote devices on the same network and then filter to register. It is useful if you do not know the exact IP address.
Manual Add	Enter the IP address, user name and password of remote device. For some remote devices, you can enter IP address, user name, and password to register.
Batch add (by CSV template)	Fill in information about remote device in the template, import the template to add the device. For batch adding, when IP address, user name and other information of remote device is inconsistent, it is suggested to use this mode.

6.2.1.1 Adding by Search

Step 1 Click ⚙, and then select **DEVICE**.

Step 2 Click + or **Add**, and then select **Smart Add**.

Figure 6-7 Smart add



Add Device ×

Smart Add | Manual Add | RTSP | Batch Import

▶ Start Search | Password | Initialize | Modify IP

☐ (1)	Initialization State	Address	Product Model	Manufacturer	Port	Product Type	Sn	Operate
☑	✓ Initialized	[redacted]	[redacted]148S	Onvif	80	--	--	⚙ LIVE
☐	✓ Initialized	[redacted]	[redacted]	Onvif	80	--	--	⚙ LIVE
☐	✓ Initialized	[redacted]	[redacted]SR_2	Onvif	80	--	--	⚙ LIVE
☐	✓ Initialized	[redacted]	[redacted]SR_2	Onvif	80	--	--	⚙ LIVE
☐	✓ Initialized	[redacted]	[redacted]136S	Private	37777	[redacted]	4M04994YA...	⚙ LIVE
☐	✓ Initialized	[redacted]	[redacted]136S	Private	37777	[redacted]	4M04994YA...	⚙ LIVE
☐	✓ Initialized	[redacted]	[redacted]136S	Private	37777	[redacted]	4M04994YA...	⚙ LIVE
☐	✓ Initialized	[redacted]	[redacted])116	Private	37777	[redacted]	1.000.0000.0.R	⚙ LIVE

Total 8 Item(s) Show up to 50 ▾ « ‹ 1/1 › » GO

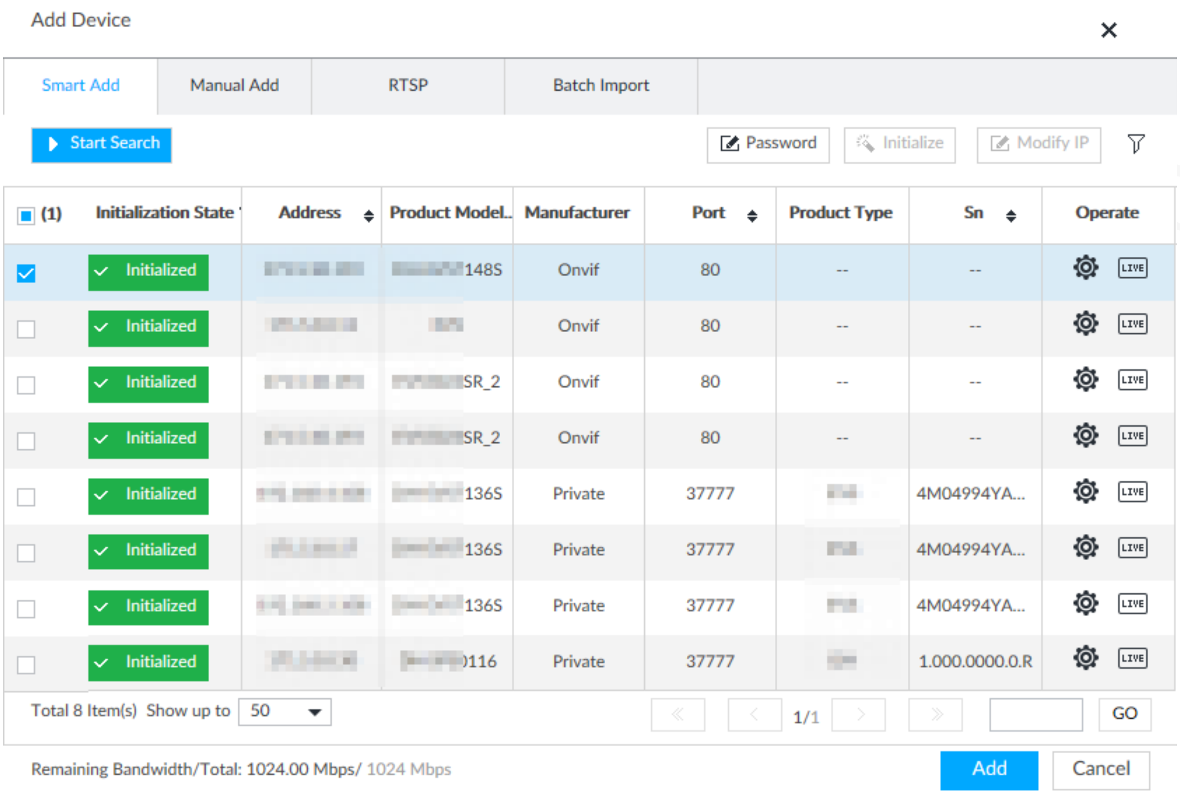
Remaining Bandwidth/Total: 1024.00 Mbps/ 1024 Mbps

Add | Cancel

Step 3 Click **Start Search**.

To set search conditions, you can click ▽.

Figure 6-8 Search results



Add Device ✕

☑ (1)	Initialization State	Address	Product Model	Manufacturer	Port	Product Type	Sn	Operate
☑	✓ Initialized	[redacted]	[redacted]148S	Onvif	80	--	--	⚙ LIVE
□	✓ Initialized	[redacted]	[redacted]	Onvif	80	--	--	⚙ LIVE
□	✓ Initialized	[redacted]	[redacted]SR_2	Onvif	80	--	--	⚙ LIVE
□	✓ Initialized	[redacted]	[redacted]SR_2	Onvif	80	--	--	⚙ LIVE
□	✓ Initialized	[redacted]	[redacted]136S	Private	37777	[redacted]	4M04994YA...	⚙ LIVE
□	✓ Initialized	[redacted]	[redacted]136S	Private	37777	[redacted]	4M04994YA...	⚙ LIVE
□	✓ Initialized	[redacted]	[redacted]136S	Private	37777	[redacted]	4M04994YA...	⚙ LIVE
□	✓ Initialized	[redacted]	[redacted]0116	Private	37777	[redacted]	1.000.0000.0.R	⚙ LIVE

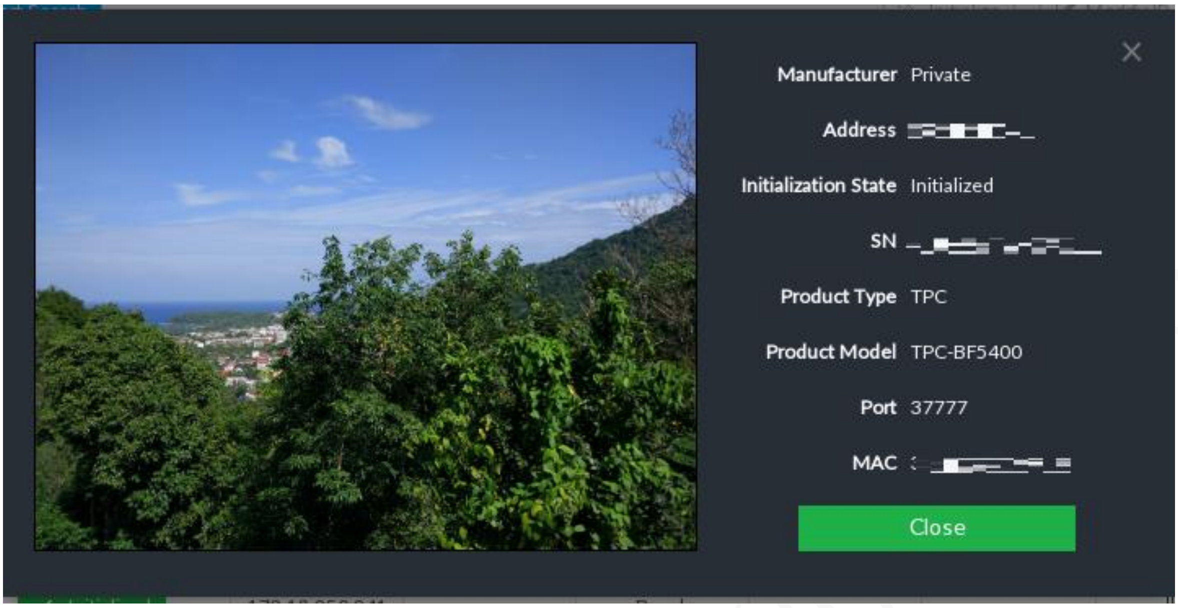
Total 8 Item(s) Show up to 50

Remaining Bandwidth/Total: 1024.00 Mbps/ 1024 Mbps

Table 6-2 Result description

Parameters	Description
Start Search	Click **Start Search** to **Start Search**ing remote device. Now it becomes **StopSearch** button. Click **StopSearch** button to stop searching remote device.
Password	Enter the username and password of the selected device.
Initialize	Select uninitialized remote device and then click **Initialize** button to initialize remote device.
Modify IP	Modify device IP address.
Initialization State	Displays remote device initialization status. Click ▾ to filter initialized or uninitialized remote device.
Operation	Click LIVE to display real-time video from the remote device. Click ☒ or **Close** to close the real-time preview window. You can view the live video if admin password of the remote device is admin, or remote device admin password is the same as the system.
Bandwidth	Displays bandwidth remaining and the total bandwidth.

Figure 6-9 Live view



Manufacturer Private

Address [redacted]

Initialization State Initialized

SN [redacted]

Product Type TPC

Product Model TPC-BF5400

Port 37777

MAC [redacted]

Step 4 Adding a remote device.

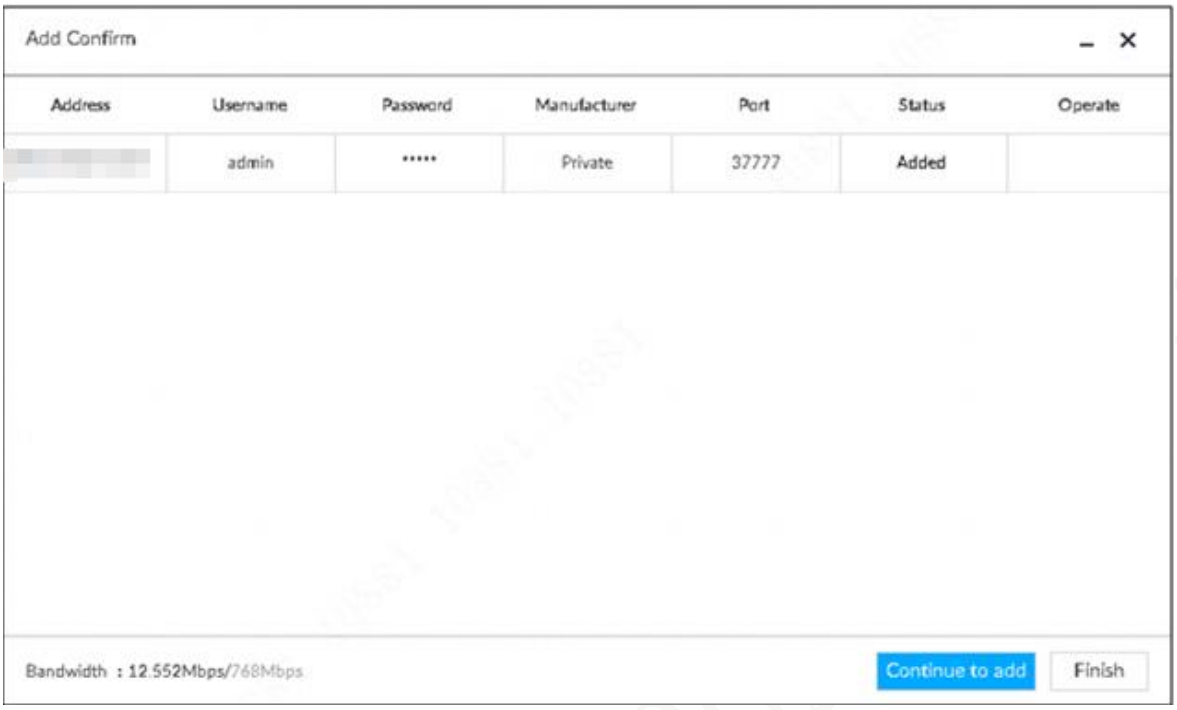
Select a remote device, click **Password**, and then enter the username and password of the selected device. Click **OK**.

- If you do not enter device username and password, the system will try to add the device by using the username and password of the current EVS.
- During the adding process, click **Cancel** button, you can cancel adding process. Click **Stop** button of the corresponding remote device to cancel add.

Step 5 Click **Add**.

- Double-click remote device IP address, user name, password, manufacturer, port to change corresponding information.
- If system fails to add the remote device, see the reason on the **Status** column to change the remote device information and then click **Retry** to try to add again.
- If a remote device is exception due to network disconnection other reasons, it can also be added. It comes online after the exception is resolved.

Figure 6-10 Confirm



Add Confirm

Address	Username	Password	Manufacturer	Port	Status	Operate
[redacted]	admin	*****	Private	37777	Added	

Bandwidth : 12.552Mbps/768Mbps

Step 6 Click **Continue to add** or **Finish**.

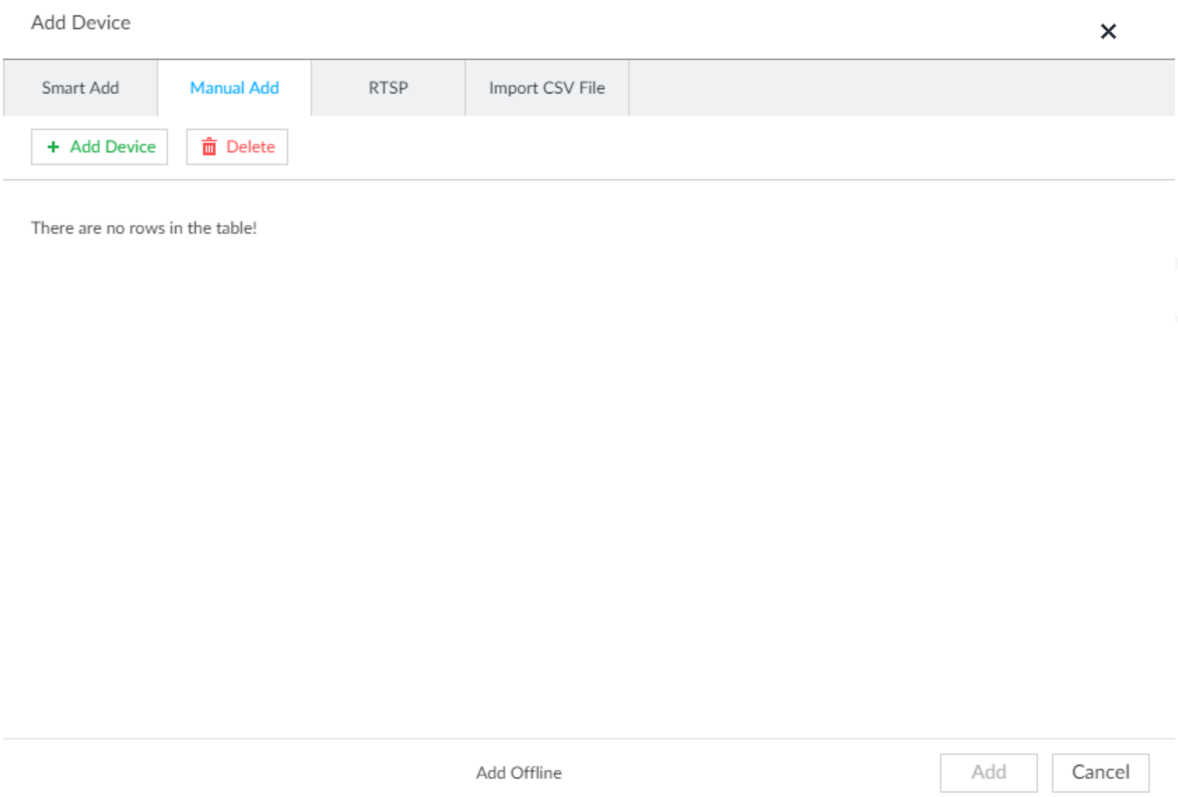
- Click **Continue to add**, device goes back to the **Smart Add** interface to add more remote device.
- Click **Finish** to complete adding remote device process. Device displays **Device** interface to view the newly added remote device information.

6.2.1.2 Adding Manually

Step 1 Click ⚙, and then select **DEVICE**.

Step 2 Click + and then select **Manual add**.

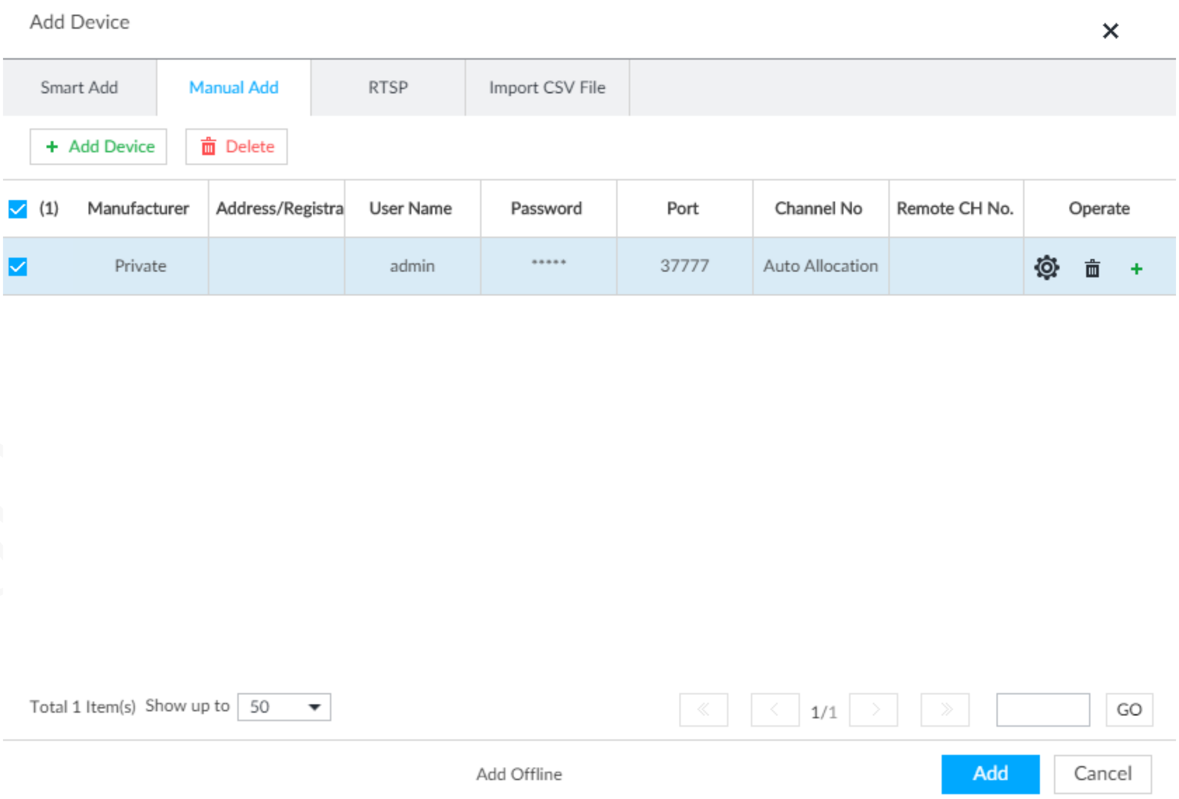
Figure 6-11 Adding manually



There are no rows in the table!

Step 3 Click **Add Device**.

Figure 6-12 Adding device



☑ (1)	Manufacturer	Address/Registra	User Name	Password	Port	Channel No	Remote CH No.	Operate
☑	Private		admin	*****	37777	Auto Allocation		⚙ 🗑 +

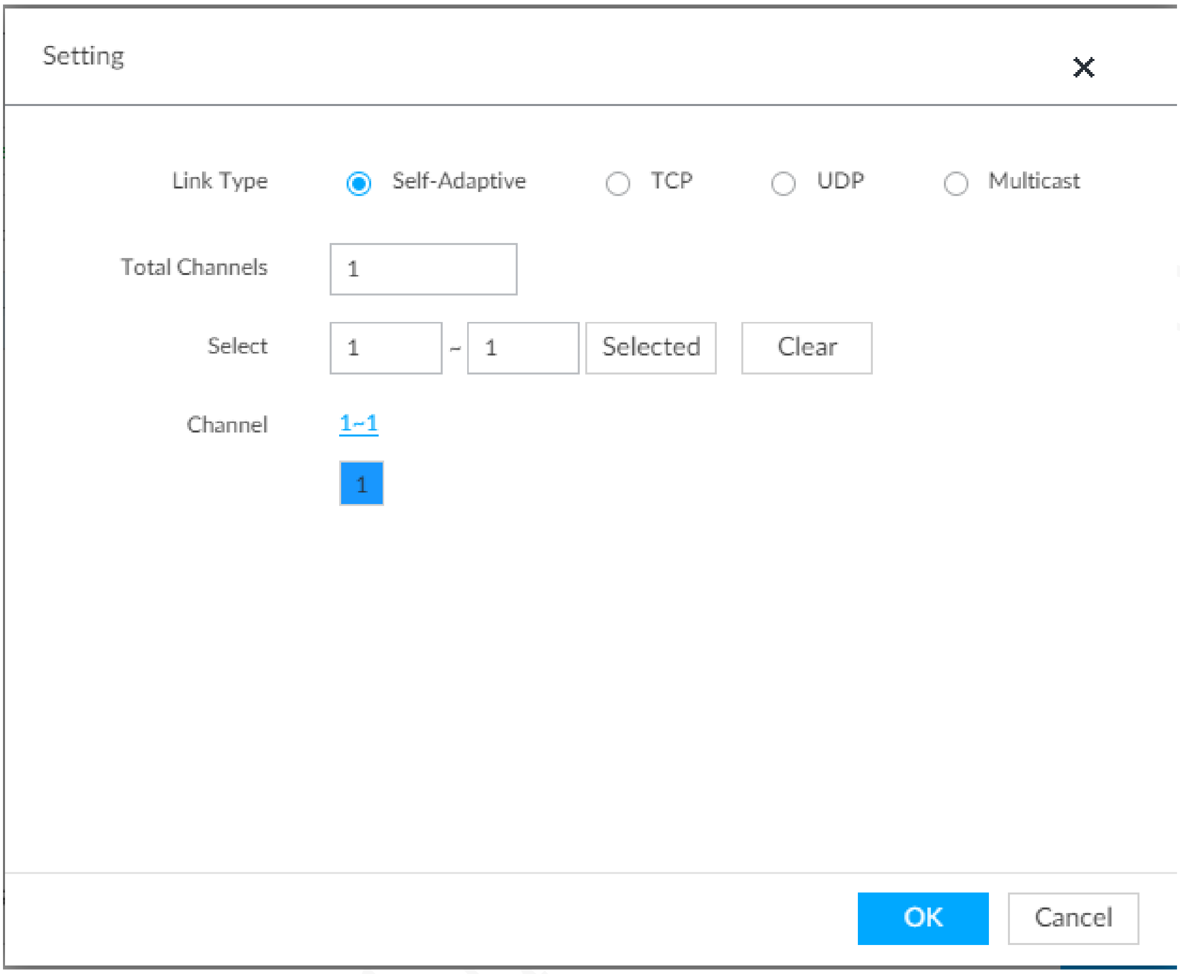
Total 1 Item(s) Show up to 50

Step 4 Set parameters.

Table 6-3 Parameters

Parameters	Description
Manufacturer	Displays the connection protocol of the remote device. Default protocol of the system is **Private**. Double-click **Private** to select other protocols. To add stream media device, select RTSP protocol, and enter RTSP address of stream media device in the **Address/Register** column. ● Port: Enter port number. The default setting is 554. ● Channel: Enter channel number of the stream media device to be added. ● Subtype: Set record bit stream type. It includes main stream 0 and sub stream 1. For example: rtsp://admin:admin@192.168.20.25:554/cam/realmonitor?channel=1&subtype=0. To add a stream media device, it is unnecessary to set user name, password, and port.
Address/Registration IP	Double-click the empty cell in the **Address/Registration** IP column to enter the IP address or RTSP address of remote device.
Username	Double-click the empty cells in the **User Name** and **Password** columns to enter the username and password of remote device.
Password	
Port	Displays the default port number of remote device. If the port number has been modified, double-click the port cell to enter the current port number of the remote device.
Channel No.	Double-click this column to select the channel number of the device in IVSS. If you select **Auto Allocation**, IVSS will provide a channel number automatically.
Remote CH No.	Select the channel number of a remote device.
Others	Delete current line or add a new line. ● Click 🗑 to delete current line information. Select multiple lines of remote device information, and then click **Delete** to batch delete the selected information. ● Click + to add a new line. Enter remote device information to add several devices at the same time.

Figure 6-13 Setting



Setting

Link Type: ● Self-Adaptive ○ TCP ○ UDP ○ Multicast

Total Channels: 1

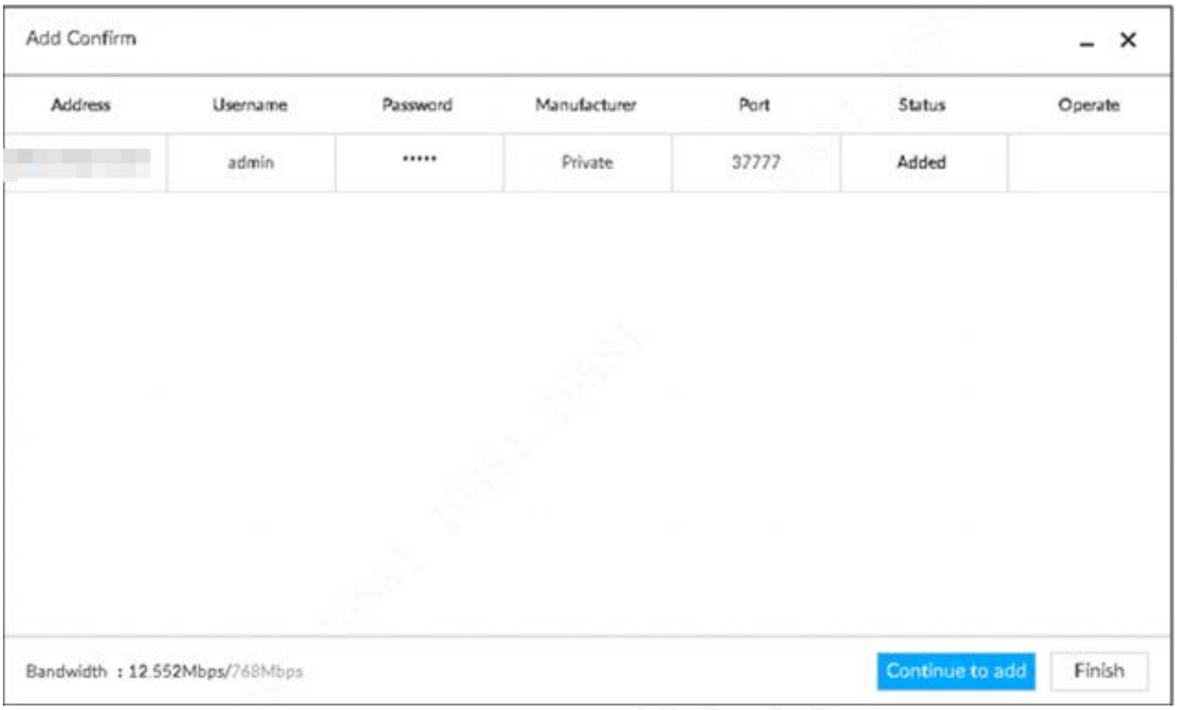
Select: 1 ~ 1

Channel: 1~1

Step 5 Select the remote device and then click **Add**. Device begins adding remote device and pops up the confirmation interface.

- During the adding process, click **Cancel** button, you can cancel adding process. Click **Stop** button of the corresponding remote device to cancel.
- Double-click remote device IP address, user name, password, manufacturer, port to change corresponding information.
- If system fails to add the remote device, see the reason on the **Status** column to change the remote device information and then click **Retry** to try to add again.
- If a remote device is exception due to network disconnection other reasons, it can also be added. It comes online after the exception is resolved.

Figure 6-14 Confirm



Add Confirm

Address	Username	Password	Manufacturer	Port	Status	Operate
[redacted]	admin	*****	Private	37777	Added	

Bandwidth ：12.552Mbps/768Mbps

Step 6 Click **Continue to add** or **Finish**.

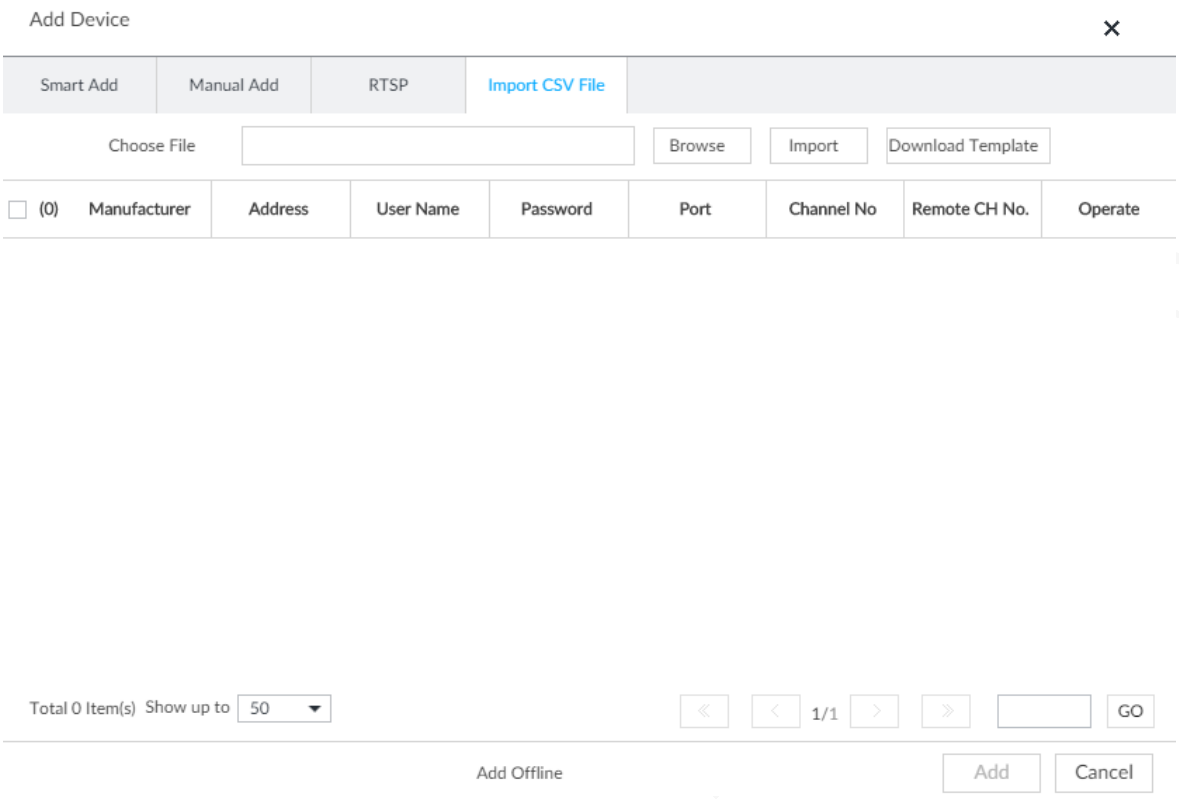
- Click **Continue to add**, device goes back to **Smart add** interface to add more remote device.
- Click **Finish** to complete adding remote device process. Device displays **Device** interface to view the newly added remote device information.

6.2.1.3 Adding in Batches

Step 1 Click ⚙, and then select **DEVICE**.

Step 2 Click +, and then select **Import CSV file** tab.

Figure 6-15 Importing CSV file



<u>Step 3</u> Fill in template file.

1) Click **Download Template** to download template file.

   File path might vary depending on interface operations, and the actual interface shall prevail.

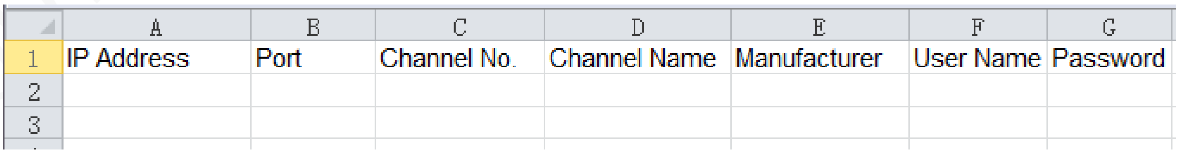
   - At PCAPP, click ≡, select Download content to view file saving path.
   - Select file saving path during local operation.
   - During web operations, files are saved under default downloading path of the browser.

2) Fill in template file and save according to your actual situation.

   The following information of template file shall be filled in.

   If information about remote device is not filled in completely, improve it after importing template.

Figure 6-16 File



	A	B	C	D	E	F	G
1	IP Address	Port	Channel No.	Channel Name	Manufacturer	User Name	Password
2							
3							

<u>Step 4</u> Import template file.

1) Click **Browse** to select the upgrade file.
2) Click **Import**.

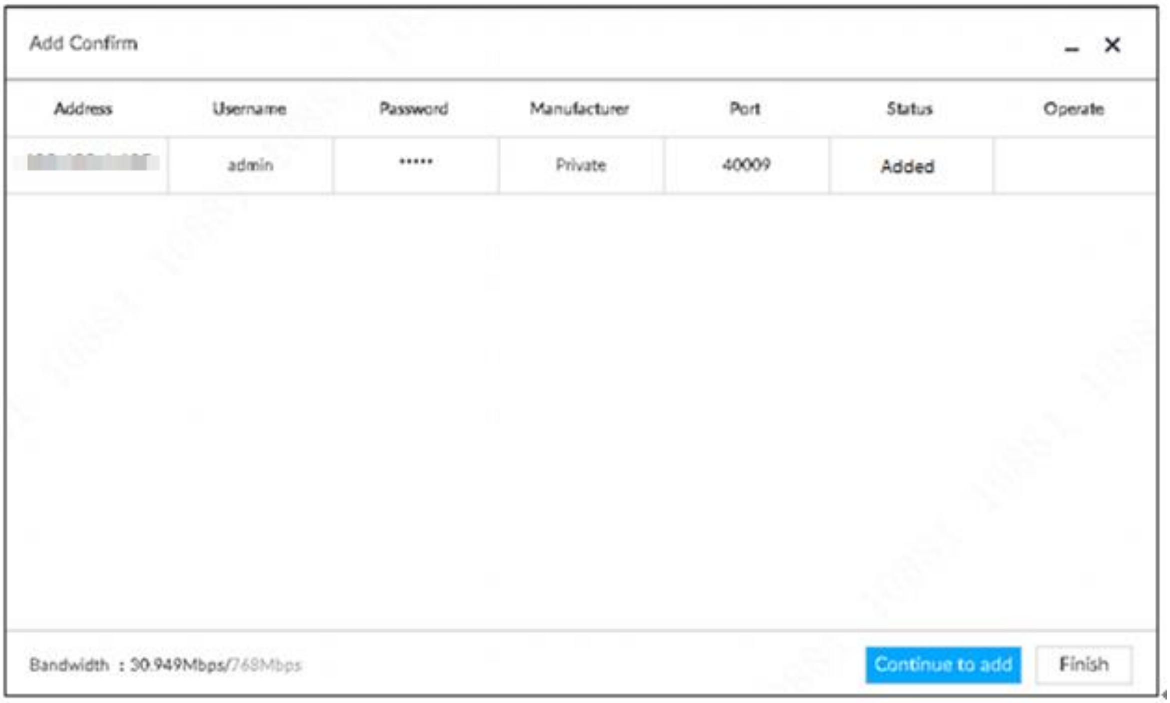
- When information about remote device is incomplete, complement it according to your actual situation.
- Click 🗑 to delete current line information.

Step 5 Add remote devices.

Select the remote device and then click **Add**. Device begins adding remote device and pops up confirmation interface.

- During the adding process, click **Cancel** button, you can cancel adding process. Click **Stop** button of the corresponding remote device to cancel add.
- Double-click remote device IP address, user name, password, manufacturer, port to change corresponding information.
- If system fails to add the remote device, see the reason on the **Status** column to change the remote device information and then click **Retry** to try to add again.

Figure 6-17 Confirm



Add Confirm

Address	Username	Password	Manufacturer	Port	Status	Operate
[redacted]	admin	*****	Private	40009	Added	

Bandwidth : 30.949Mbps/768Mbps

Step 6 Click **Continue to add** or **Finish**.

- Click **Continue to add**, device goes back to **Smart add** interface to add more remote device.
- Click **Finish** to complete adding remote device process. Device displays **Device manager** interface to view the newly added remote device information.

Step 7 (Optional) You can add offline devices when the network is exception. When the network recovers, the added offline device will automatically come online.

Click ▭ next to offline device to add an offline device.

Step 8 (Optional) Click ▭ next to **Overwrite** to enable the function. This function is used when the IP address of a new device is the same as that of a previously added device, the configuration of the new device will overwrite the old one.

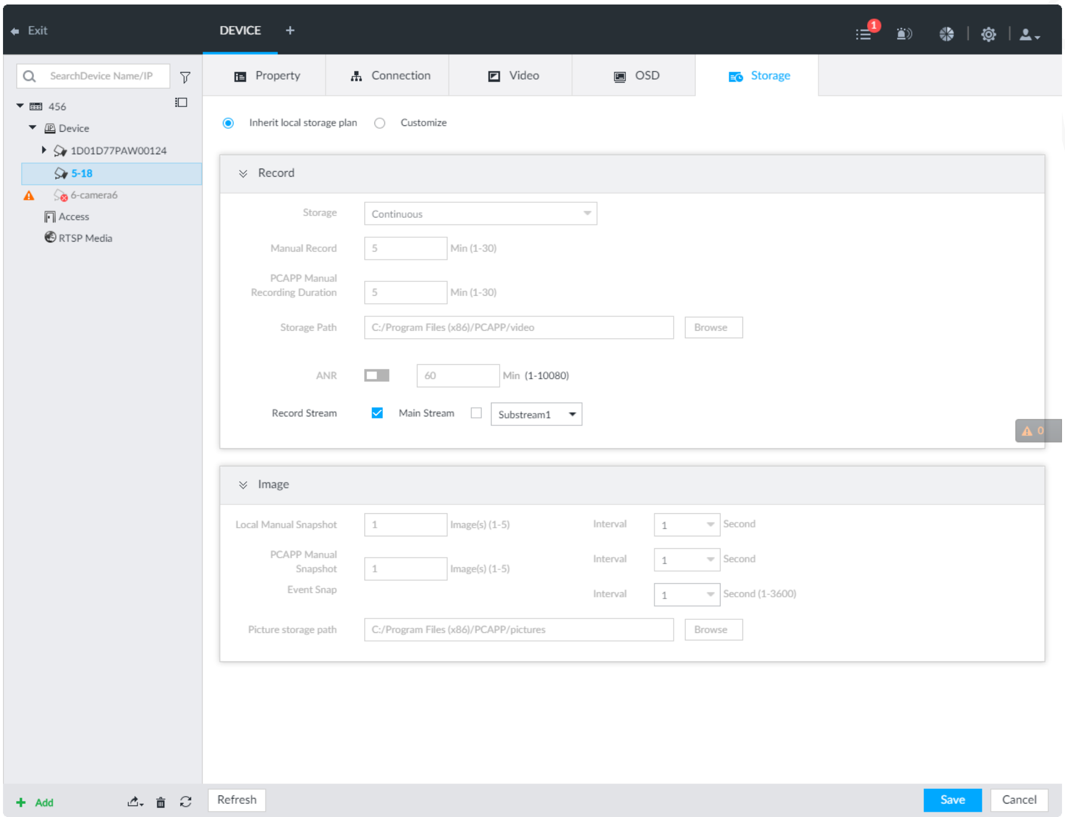
6.2.2 Configuring Storage Plan on IVSS

Set TPC video and image storage plan on IVSS according to the actual situation.

Step 1 Click ⚙, or click + on the configuration interface, and then select **DEVICE**.

Step 2 Select a remote device on the left panel and then click **Storage** tab.

Figure 6-18 Storage



● Inherit local storage plan ○ Customize

Record

Storage: Continuous

Manual Record: 5 Min (1-30)

PCAPP Manual Recording Duration: 5 Min (1-30)

Storage Path: C:/Program Files (x86)/PCAPP/video Browse

ANR: 60 Min (1-10080)

Record Stream: ☑ Main Stream □ Substream1

Image

Local Manual Snapshot: 1 Image(s) (1-5) Interval: 1 Second

PCAPP Manual Snapshot: 1 Image(s) (1-5) Interval: 1 Second

Event Snap: Interval: 1 Second (1-3600)

Picture storage path: C:/Program Files (x86)/PCAPP/pictures Browse

Step 3 Select **Inherit local storage plan** or **Customize**.

- **Inherit local storage plan**: The remote device adopts global storage plan of the Device.
- **Customize**: Set customized storage plan.

Step 4 Set parameters.

Set record streams only if you select **Inherit local storage plan**.

Table 6-4 Storage parameters description

Parameters		Description
Record	Storage	Set record strategy. ● Continuous Recording: 24-hour continuous recording. ● Not Recording: Device is not recording. ● Event Recording: Device only records when there is corresponding alarm event. ● Scheduled: Record in the scheduled time. ● Scheduled & Event: Record in the scheduled time and also on the basis of event-triggering.
	ANR	● When a camera gets disconnected with IVSS, it stores the recorded videos in its local SD card. When the camera is connected again, it will upload the video during the disconnection to IVSS. ● Set the maximum length of the to-be-uploaded video so that after getting reconnected, the camera will only upload video of the pre-defined length to IVSS. Make sure that the camera has an SD card.
	Manual Record (length)	Set manual record file length. On the **LIVE** interface, click ▣ to start record. If you do not click the icon to stop record, system stops recording automatically according to the record length here.
	PCAPP Manual Recording Duration	Set the time length of manual recording performed on the PCAPP client. Click ▣ to start manual recording on the PCAPP client. The manual recording automatically finishes at the end of the pre-defined time period.
	Storage Path	Click **Browser** to set manual record storage path. Only PCAPP supports this function.
Image	Local Manual Snapshot	It is to set manual snapshot amount and snapshot speed.

Parameters		Description
	Event Snap	It is to set event snapshot interval. Select **Customize** to set customized interval. The maximum internal is 3600 seconds.
	Picture storage path	Click **Browser** to set snapshot image storage path. 📖 Only PCAPP supports this function.

Step 5 Click **Save**.

6.2.3 Configuring Mask Detection

Configure face mask alarm so that an alarm is triggered when a person is detected not wearing face mask.

6.2.3.1 Enabling Face Detection

Enable face detection or recognition, whether AI by camera or AI by device, before configuring face mask detection. Take enabling face detection with AI by device for example.

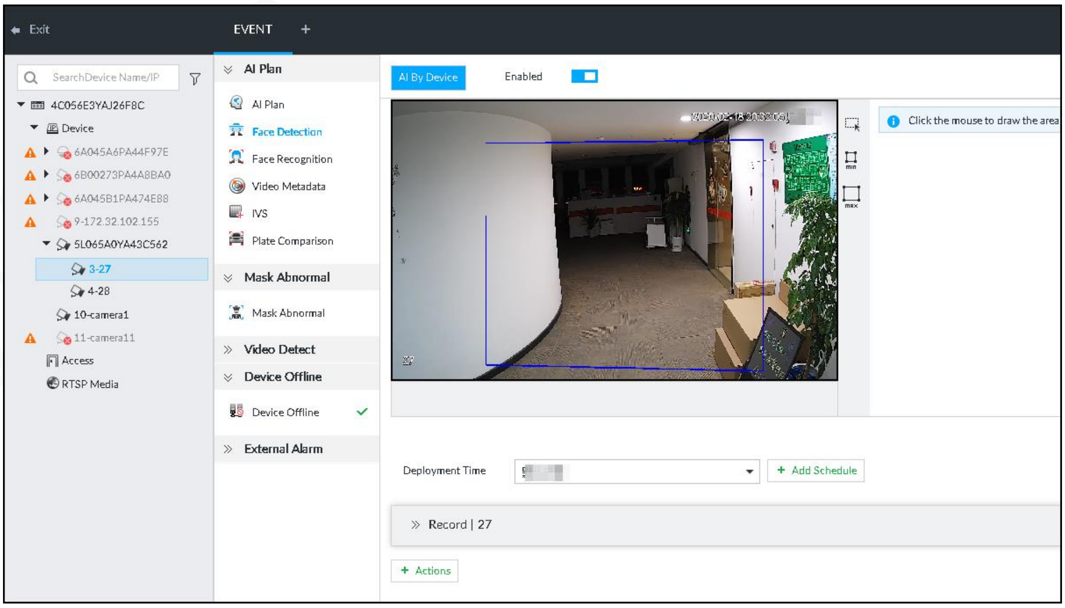
Step 1 Log in to PCAPP.

Step 2 Click ⚙, then select **EVENT**.

Step 3 On the device tree, select a thermal camera channel, and then select **AI Plan** > **Face Detection**.

Step 4 Click ▭ to enable face detection.

Figure 6-19 Face detection



Step 5 Click **Save**.

6.2.3.2 Configuring Mask Abnormal Alarm

Step 1 Log in to PCAPP.

Step 2 Click ⚙, then select **EVENT**.

Step 3 On the device tree, select a thermal camera channel, and then select **Mask Abnormal** > **Mask Abnormal**.

Step 4 Click ▭ next to **Mask Abnormal** to enable the function.

Step 5 Click ▭ next to **Show Feature Panel** to enable feature panel.

When a person is detected not wearing face mask, the detection result will be displayed on the live view.

Step 6 Configure alarm actions.

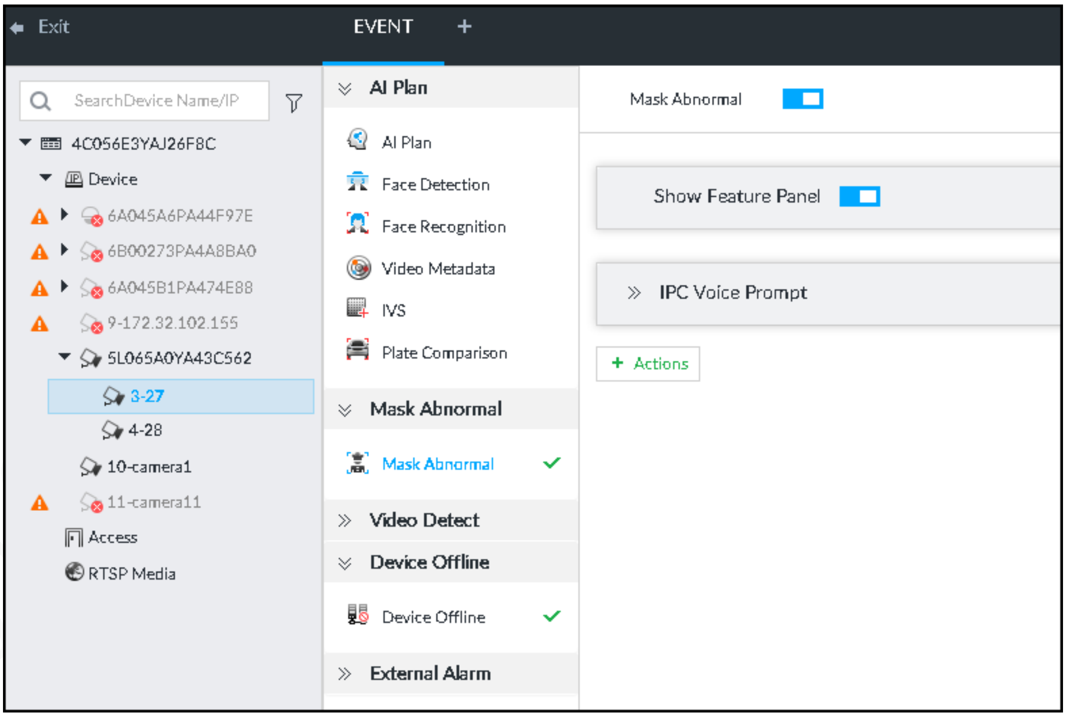
You can configure alarm actions such as video recording, snapshot, buzzer, local voice prompt, IPC voice prompt, IPC alarm out, local alarm out, IPC white light (for warning), preset and email. Take configuring IPC voice prompt for example.

📖

To configure IPC voice prompt, make sure that the camera has audio files. On the **IPC Voice Prompt** interface, click **Remote Voice Manage** to import audio file.

1) Click **Actions**, and then select **IPC Voice Prompt**.
2) Select the camera for voice prompt, and then select the audio file.

Figure 6-20 Mask abnormal



Step 7 Click **Save**.

6.3 Configuring NVR

Skip this chapter if you do not have NVR in your product combination.

6.3.1 Adding TPC to NVR

You can add cameras to NVR and manage them remotely.

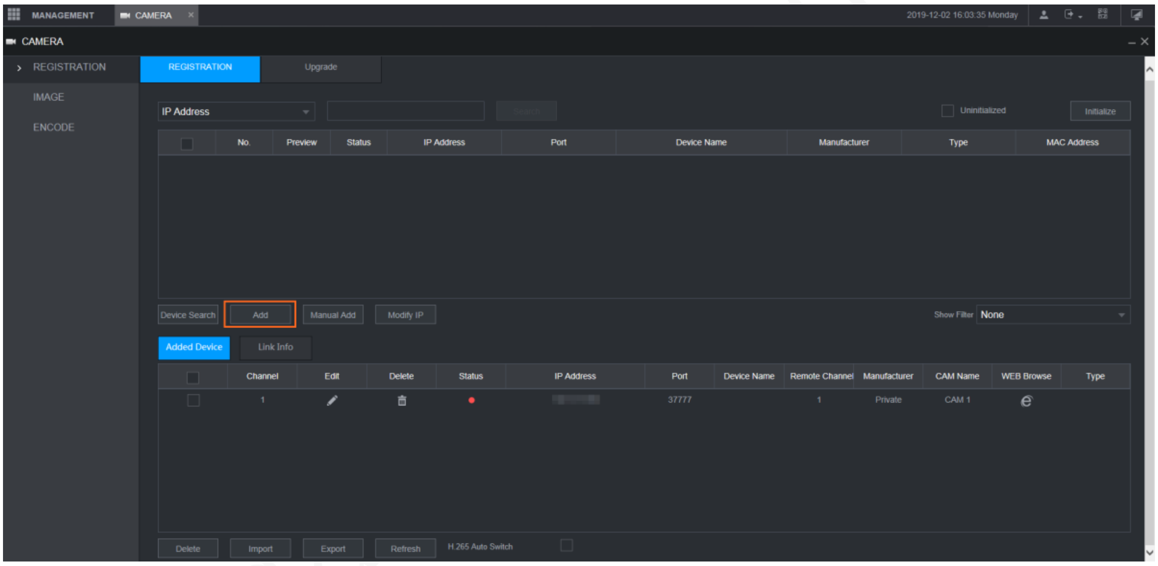
Preparation

- For brand new NVR, see the quick start guide or user's manual to initialize it and modify IP address.
- For NVR that are properly configured, be sure to update the system to the latest version.

Procedure

Step 1 Log in to the NVR web interface, and then select **MANAGEMENT > CAMERA > REGISTRATION**.

Figure 6-21 Camera (1)



□	No.	Preview	Status	IP Address	Port	Device Name	Manufacturer	Type	MAC Address

□	Channel	Edit	Delete	Status	IP Address	Port	Device Name	Remote Channel	Manufacturer	CAM Name	WEB Browse	Type
□	1	✎	🗑	●	[redacted]	37777		1	Private	CAM 1	e	

Step 2 Add devices.

You can add cameras with auto scan and manual add.

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

- Auto scan

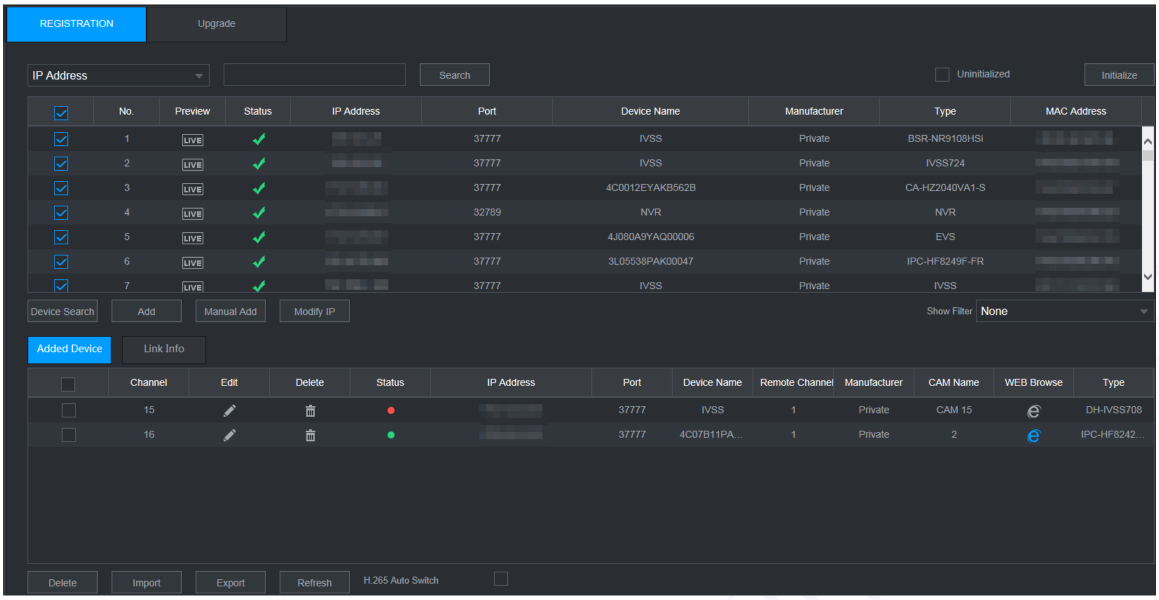
1) Click Device Search.

The devices searched will be displayed.

2) Double-click the device information or select the check box before it, and then click **Add**, the device will be added to the list of added devices.

You can refresh the list of added devices to avoid adding the same camera repeatedly.

Figure 6-22 Camera (2)



☑	No.	Preview	Status	IP Address	Port	Device Name	Manufacturer	Type	MAC Address
☑	1	LIVE	✓	[redacted]	37777	IVSS	Private	BSR-NR9108HSi	[redacted]
☑	2	LIVE	✓	[redacted]	37777	IVSS	Private	IVSS724	[redacted]
☑	3	LIVE	✓	[redacted]	37777	4C0012EYAKB562B	Private	CA-HZ2040VA1-S	[redacted]
☑	4	LIVE	✓	[redacted]	32789	NVR	Private	NVR	[redacted]
☑	5	LIVE	✓	[redacted]	37777	4J080A9YAQ00006	Private	EVS	[redacted]
☑	6	LIVE	✓	[redacted]	37777	3L05538PAK00047	Private	IPC-HF8249F-FR	[redacted]
☑	7	LIVE	✓	[redacted]	37777	IVSS	Private	IVSS	[redacted]

□	Channel	Edit	Delete	Status	IP Address	Port	Device Name	Remote Channel	Manufacturer	CAM Name	WEB Browse	Type
□	15	✎	🗑	🔴	[redacted]	37777	IVSS	1	Private	CAM 15	e	DH-IVSS708
□	16	✎	🗑	🟢	[redacted]	37777	4C07B11PA...	1	Private	2	e	IPC-HF8242...

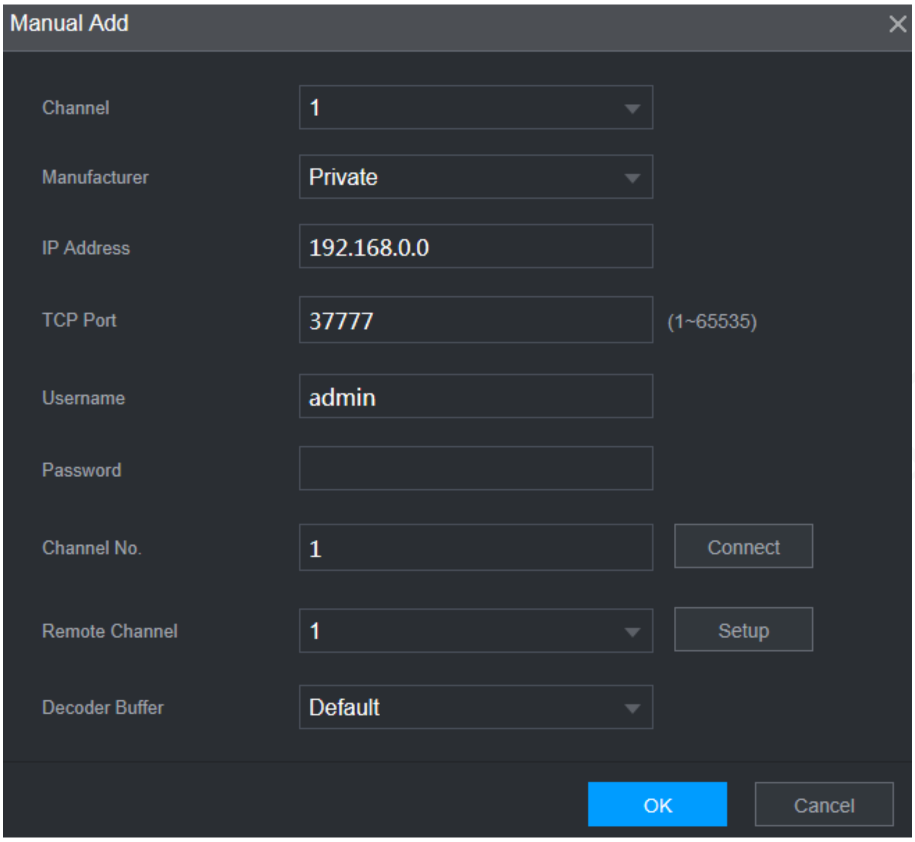
Table 6-5 Parameter description

Icon/Parameter	Description
Channel	Displays the channel No. on your NVR to which you connect the target camera to.
Edit	Click ✎, or double-click the line corresponding to the device to modify device information, such as channel, manufacturer, IP address, TCP port, user name, password, remote channel No., and decode buffer.
Delete	Click 🗑 to delete the corresponding device.
Status	Shows whether a device is initialized. 🟢 means it is initialized; 🔴 means it is uninitialized.
IP Address	Shows device information such as IP address, port number, device name, channel number of camera, manufacturer, and camera name.
Port	
Device Name	
Remote Channel	
Manufacturer	
CAM Name	
Type	
Web Browse	Click e to go to the web interface of corresponding deivce.

- Manual add

3) Click Manual Add.

Figure 6-23 Manual add



Manual Add

Channel: 1

Manufacturer: Private

IP Address: 192.168.0.0

TCP Port: 37777 (1~65535)

Username: admin

Password:

Channel No.: 1

Remote Channel: 1

Decoder Buffer: Default

4) Configure parameters.

Table 6-6 Manual add parameters

Parameter	Description
Channel	Displays the channel No. on your NVR to which you connect the target camera to.
Manufacturer	Select **Private**. 📖 Supported protocol might vary with different models, and the actual product shall prevail.
IP Address	Enter the IP address of the target camera.
TCP Port	Transmission control protocol port, the value is 37777 by default.
Username/Password	Enter the user name/password of the camera you need.
Channel No.	If the target camera has already connected to another NVR, then its channel No. on that NVR is displayed here.
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.

5) Click **OK**.

6.3.2 Configuring Recording Plan on NVR

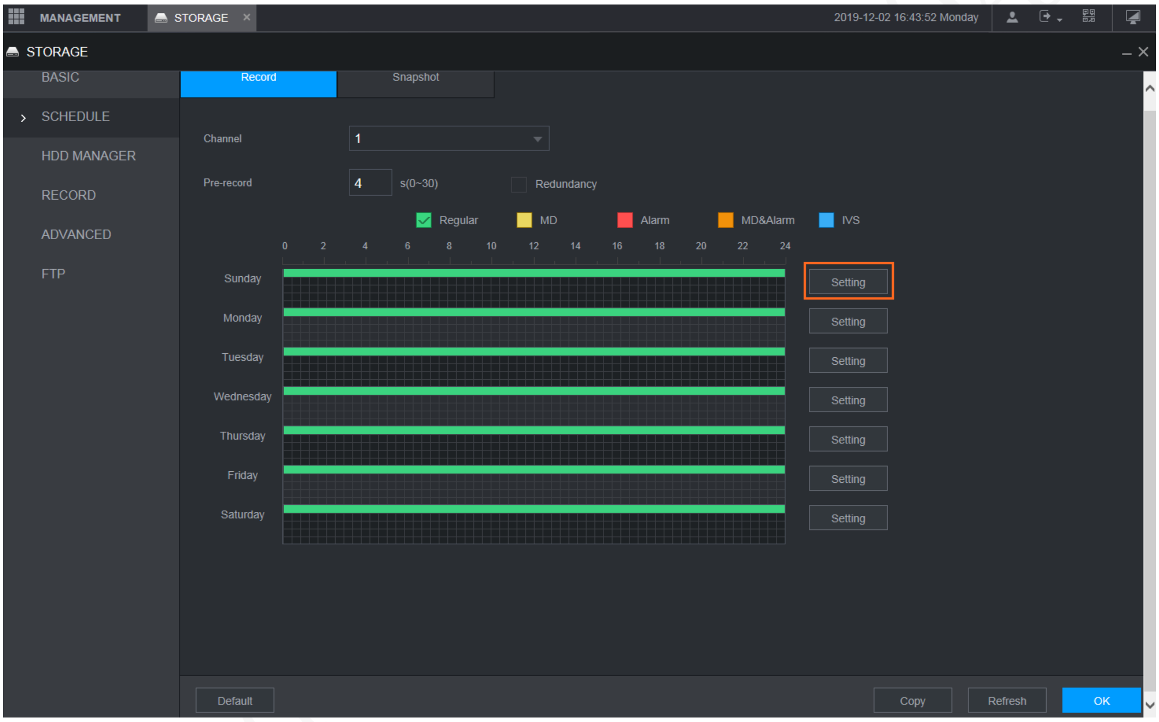
After properly configuring TPC parameters, you can save the clear videos and snapshots from the network cameras to the NVR.

⚠

Before configuring video storage, make sure that your NVR is well deployed, and HDDs are well installed and configured. For details, see NVR quick start guide and user's manual.

Step 1 Log in to the web interface of NVR, and then select **MANAGEMENT** > **STORAGE** > **SCHEDULE** > **Record**.

Figure 6-24 Record



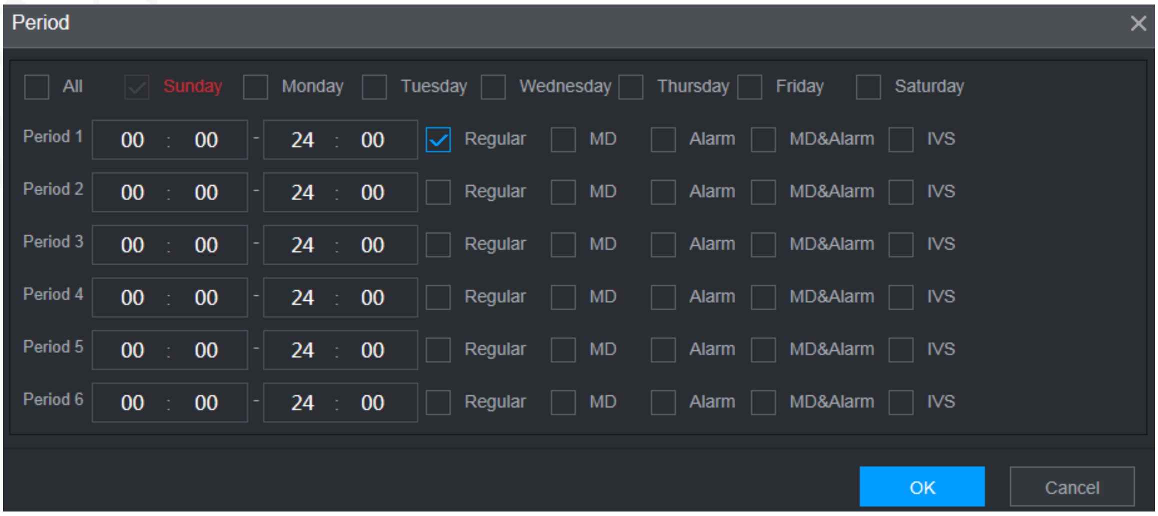
Channel: 1

Pre-record: 4 s(0~30) □ Redundancy

☑ Regular 🟨 MD 🟥 Alarm 🟧 MD&Alarm 🟦 IVS

Step 2 Select the **Channel** that you need to record, and then click **Setting** corresponding to the day that you need to configure time period.

Figure 6-25 Period



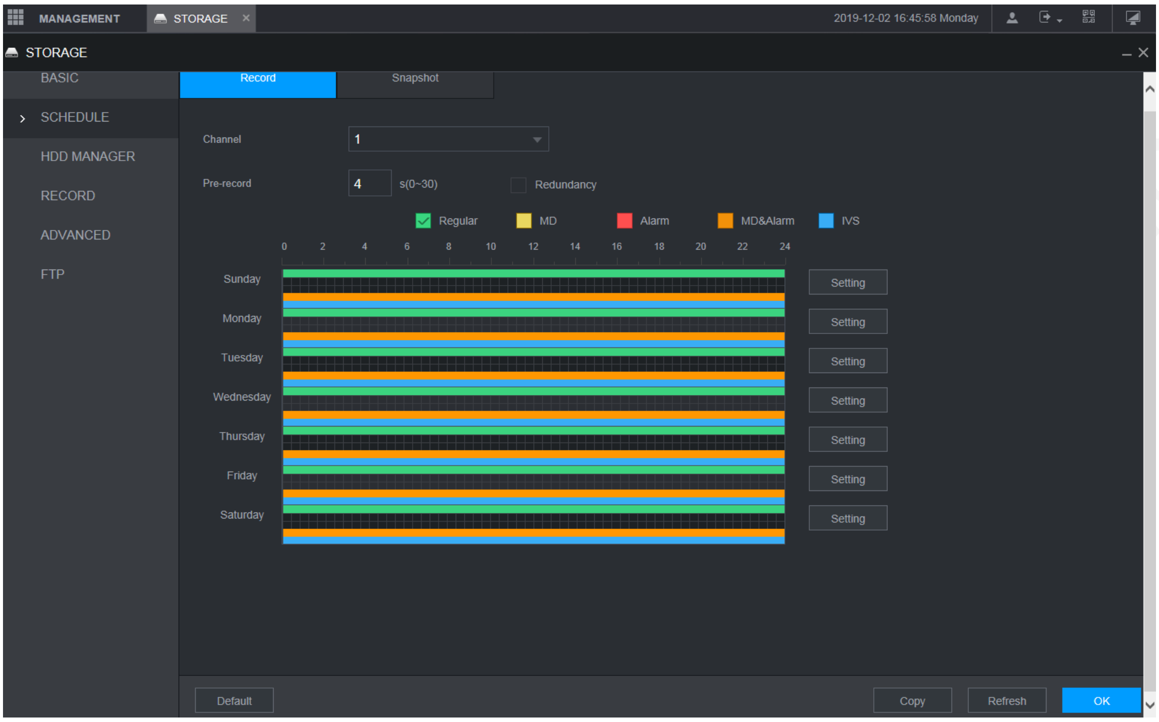
□ All ☑ Sunday □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday

Period 1	00 : 00	-	24 : 00	☑ Regular	□ MD	□ Alarm	□ MD&Alarm	□ IVS
Period 2	00 : 00	-	24 : 00	□ Regular	□ MD	□ Alarm	□ MD&Alarm	□ IVS
Period 3	00 : 00	-	24 : 00	□ Regular	□ MD	□ Alarm	□ MD&Alarm	□ IVS
Period 4	00 : 00	-	24 : 00	□ Regular	□ MD	□ Alarm	□ MD&Alarm	□ IVS
Period 5	00 : 00	-	24 : 00	□ Regular	□ MD	□ Alarm	□ MD&Alarm	□ IVS
Period 6	00 : 00	-	24 : 00	□ Regular	□ MD	□ Alarm	□ MD&Alarm	□ IVS

Step 3 Select the days you need, and if you select **All**, the defined time period would apply to the whole week. You can configure 6 time periods at most for each day.

Step 4 Select the record type for the corresponding time period, and then click **OK**.

Figure 6-26 Record plan



Channel: 1

Pre-record: 4 s(0~30)

☐ Redundancy

☑ Regular 🟨 MD 🟥 Alarm 🟧 MD&Alarm 🟦 IVS

Each color matches with a different record schedule. Green means normal videos, yellow means motion detection videos, and red means alarm videos.

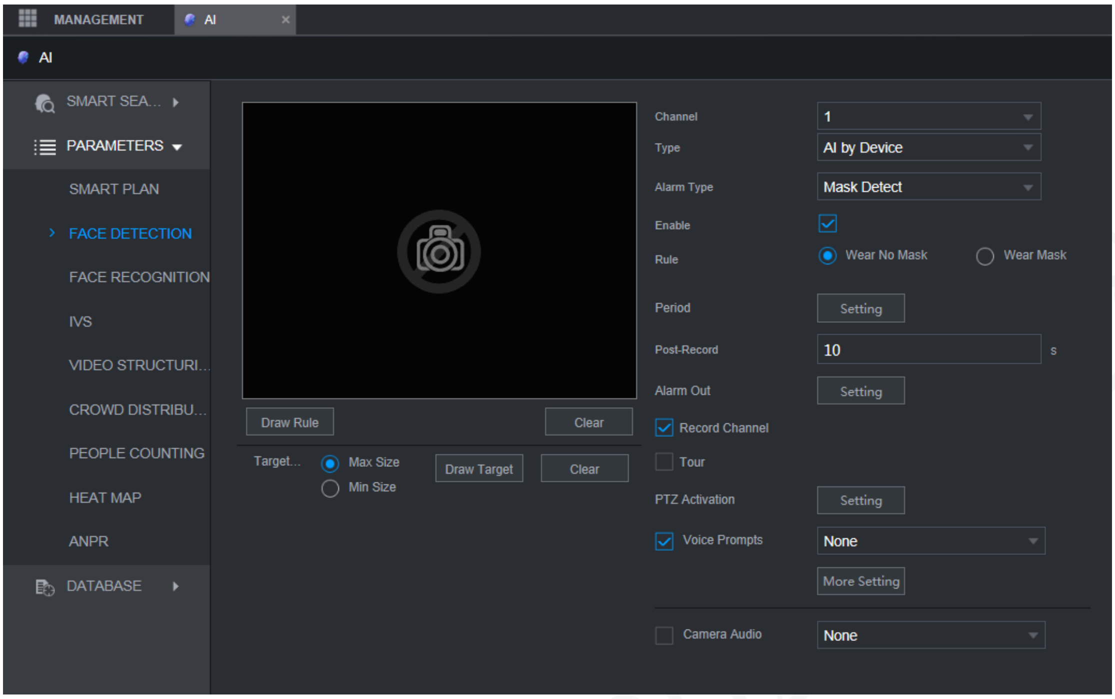
Step 5 Configure **Pre-record** duration, and then the system saves videos before any event as well. For example, if the value is 4, then the system saves videos from 5 seconds before any event starts.

Step 6 Click **OK**.

6.3.3 Configuring Mask Abnormal Alarm

Step 1 Log in to NVR, and then select **AI > PARAMETERS > FACE DETECTION**.

Figure 6-27 Configure mask abnormal detection



Channel: 1

Type: AI by Device

Alarm Type: Mask Detect

Enable: ☑

Rule: ● Wear No Mask ○ Wear Mask

Period: Setting

Post-Record: 10 s

Alarm Out: Setting

☑ Record Channel

□ Tour

PTZ Activation: Setting

☑ Voice Prompts: None

□ Camera Audio: None

Step 2 Select the target channel from the **Channel** drop-down list.

Step 3 Select **AI by Device** for **Type** and **Mask Detect** for **Alarm Type**.

Step 4 Select the **Enable** check box to enable the alarm.

Step 5 Select **Wear No Mask** for **Rule**.

Mask abnormal alarm is triggered when the system detects a person not wearing a mask.

Step 6 Click **Setting** to specify the period in which the alarm is valid. It is full period by default.

Step 7 (Optional) To enable voice prompt from the NVR, select the check box next to **Voice Prompts**. To enable audio warning from the camera, select the check box next to **Camera Audio**.

The camera audio function is only available on the camera that supports sound and light warning.

6.4 Configuring Express

After installing and activating Express, you need to add devices, configure device features, set recording plan and storage space. Skip this chapter if you do not have Express in your product combination.

6.4.1 Adding Devices to Express

You can add TPC by entering camera information, or searching the network for online TPCs to quickly add them.

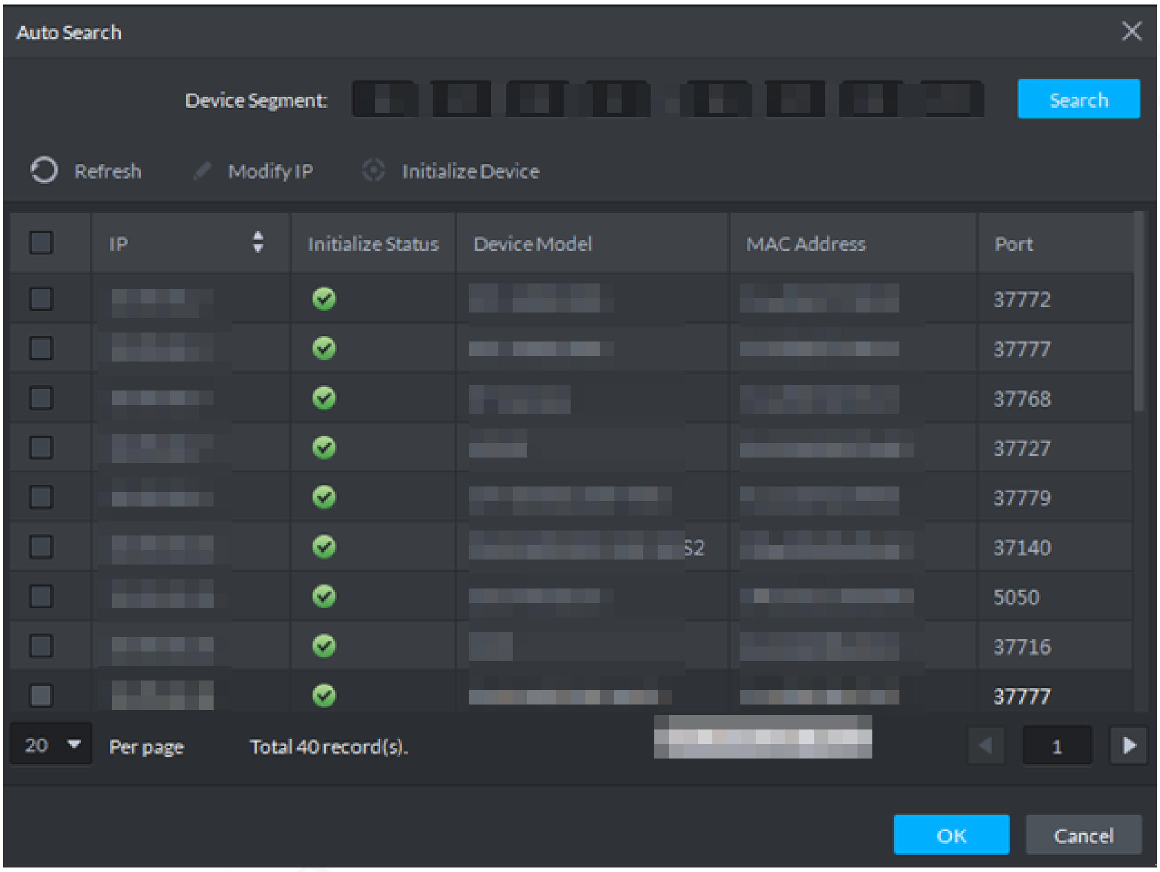
6.4.1.1 Adding by Search

Step 1 Click **Device** on the client homepage.

Step 2 Click **Auto Search**.

The system searches the device with the same segment as server by default.

Figure 6-28 Auto search



Auto Search

Device Segment: [redacted] Search

Refresh Modify IP Initialize Device

□	IP	Initialize Status	Device Model	MAC Address	Port
□	[redacted]	✓	[redacted]	[redacted]	37772
□	[redacted]	✓	[redacted]	[redacted]	37777
□	[redacted]	✓	[redacted]	[redacted]	37768
□	[redacted]	✓	[redacted]	[redacted]	37727
□	[redacted]	✓	[redacted]	[redacted]	37779
□	[redacted]	✓	[redacted]	[redacted]	37140
□	[redacted]	✓	[redacted]	[redacted]	5050
□	[redacted]	✓	[redacted]	[redacted]	37716
□	[redacted]	✓	[redacted]	[redacted]	37777

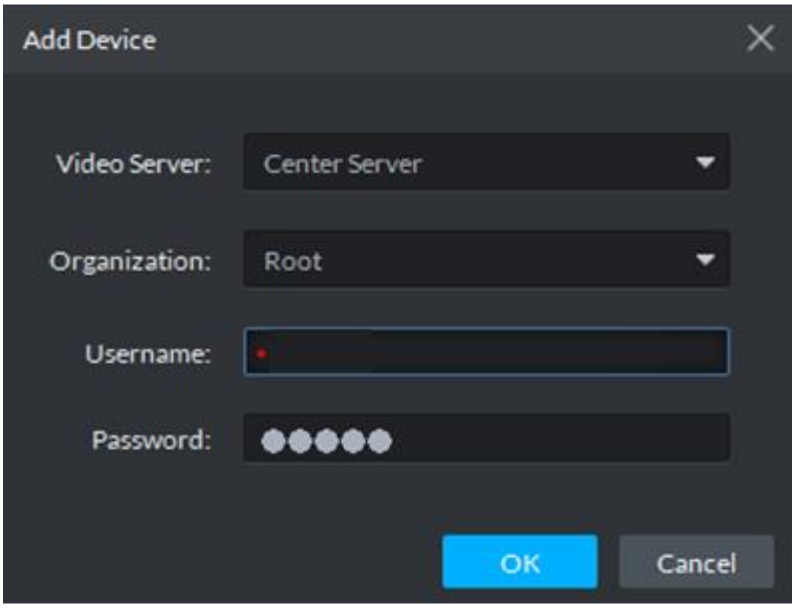
20 Per page Total 40 record(s). [redacted] 1

OK Cancel

Step 3 Enter searched start IP and end IP, click **Search**.

Step 4 Select the device to be added, click **OK**.

Figure 6-29 Add Device



Add Device

Video Server: Center Server

Organization: Root

Username:

Password: ●●●●●

OK Cancel

Step 5 Enter login username and password, click **OK**.

- The added device username is required to be the same as password when adding several devices.
- After device is added, the system continues to stay on the **Auto Search** interface, click **Cancel** or ✕ to exit interface.
- After device is added, the platform logs in device automatically, the device is displayed as online after logging in successfully. If offline, please make sure if login username and password are correct, click ✎ to modify username and password.

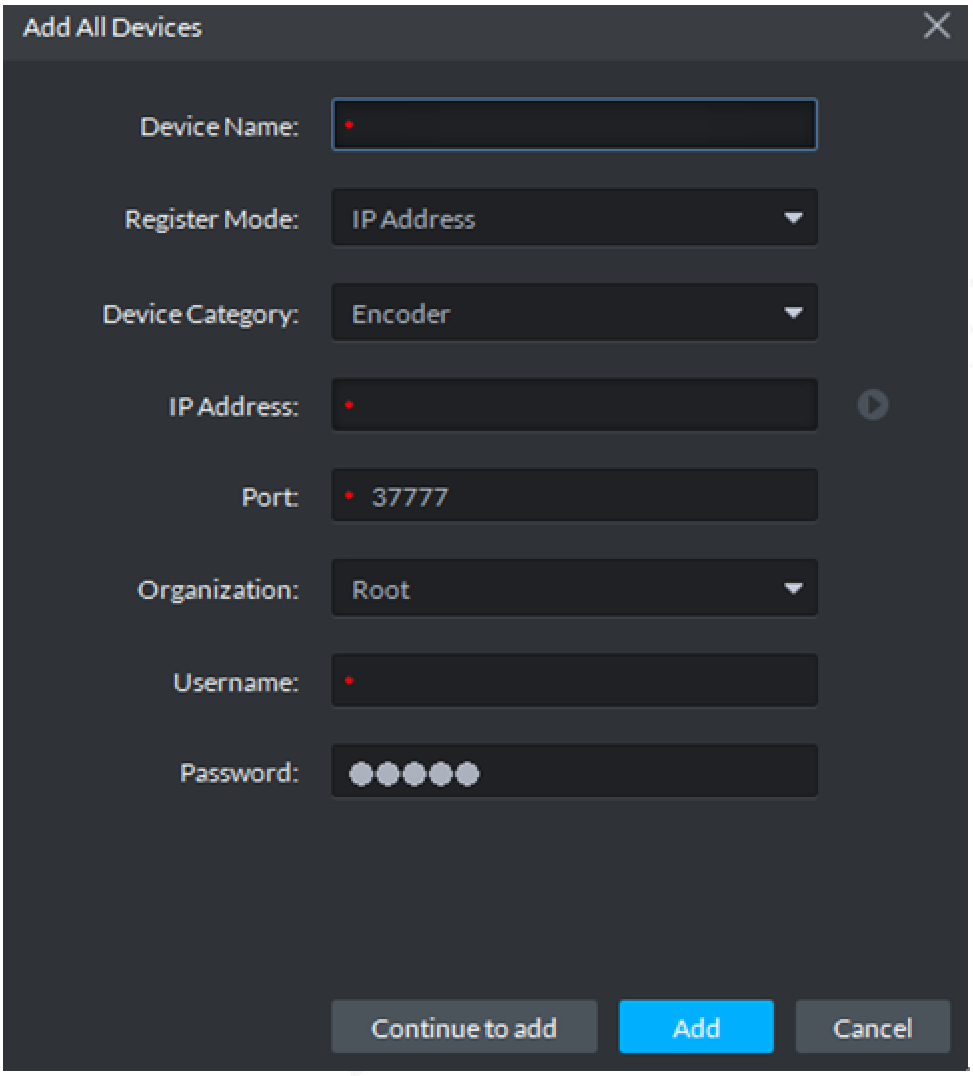
6.4.1.2 Adding Manually

Add single device, or the username and password of the added device are different, or the added device is not in the same segment.

Step 1 Click **Device** on the client homepage.

Step 2 Click **Add**.

Figure 6-30 Adding manually



Add All Devices

Device Name: *

Register Mode: IP Address

Device Category: Encoder

IP Address: *

Port: * 37777

Organization: Root

Username: *

Password: ●●●●●

Step 3 Set parameters.

- The item with * is required to be filled in. You need to set different parameters if different device are connected.
- Add encoder, set correct parameters, and click ▶ to view device video.

Table 6-7 Parameter description

Parameter	Description
Device Category	Select NVR or camera.

Register Mode	Support registration by following method: ● IP address Add device to platform by adding device IP. ● Serial number (Device with P2P function) If device supports P2P function, then you can add device to platform by adding device serial number. ● Onvif If device enables Onvif protocol, then you can add device to platform by Onvif protocol. Generally it can be used when adding third-party device.
Port	TCP protocol communication provides service port, and keeps it in accordance with added device.
Organization	Select organization node of added device.
IP Address	When register by IP address or Onvif mode, set the IP address of added device.
SN	When register by serial number mode, set the serial number of added device.
Username	Enter login username and password of added device.
Password	
Decode mode	Select according to the decode mode of added device: ● Pull Decoder extracts stream from platform by url address, the decode mode of device is pull. ● Direct Decoder extracts stream directly from encoder, the decode mode is direct for device, under this mode; you need to add decoder IP address when trusted list is added by device. ● Push VMS (Video Management Service) pushes stream directly to decoder, currently only support NVD without combination screen, the mode is not supported by matrix, video wall or NVD under combination mode.
Support Combination	Select when added device supports combination.
Picture Server	Select storage location of picture reported by ANPR.
LED Type	Support added LED including general screen and free parking screen, select corresponding device type according to the accessed device.

Step 4 Click **Add**.

Click **Continue to add** if necessary, then you can add more devices.

6.4.2 Enabling TPC Features

TPC needs to rely on its intelligent video surveillance (IVS) functions to measure human body temperature. To receive data by TPC, you need to enable TPC features on Express.

Step 1 Click **Device** on the client homepage.

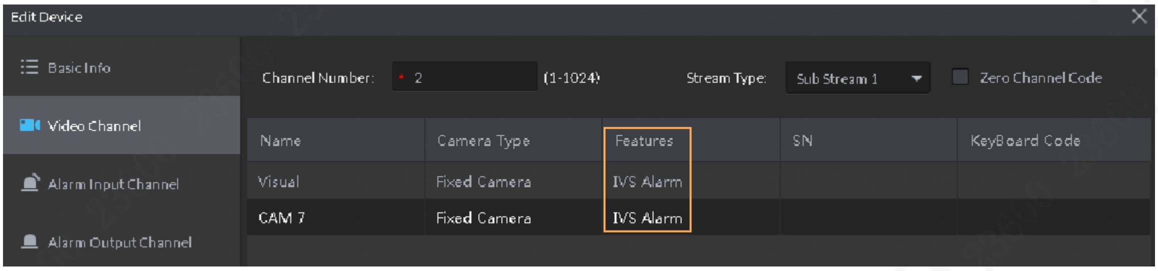
Step 2 Click ✎ next to device list.

Step 3 Click Video Channel tab.

Step 4 Select visual channel and thermal channel of TPC camera.

Step 5 Select **IVS Alarm** from the **Features** list for the two channels.

Figure 6-31 Edit device



Channel Number: 2 (1-1024) Stream Type: Sub Stream 1 □ Zero Channel Code

Name	Camera Type	Features	SN	KeyBoard Code
Visual	Fixed Camera	IVS Alarm		
CAM 7	Fixed Camera	IVS Alarm		

Step 6 Click **OK**.

6.4.3 Configuring Storage Space

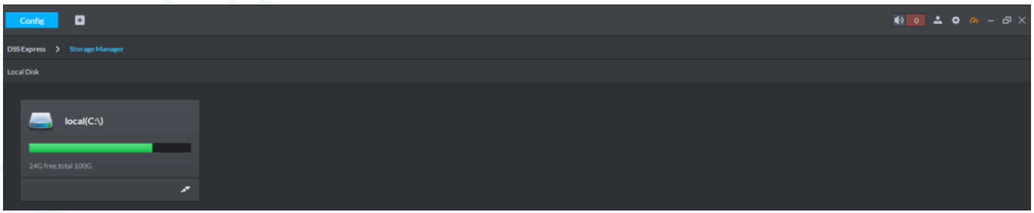
Configure the disks in the server of Express to store video and face pictures. Configure at least one disk for picture storage. When your scheme is TPC—Express, you need to configure both face image and video storage. When your scheme is TPC—IVSS/NVR—Express, you only need to configure face image storage (Video storage is optional).

Step 1 Enter configuration interface of **Storage Manager**.

1) Click **Config** on the client homepage.
2) Click **Storage**.

   The system automatically detects disk info of server (Disk info of non PC client).

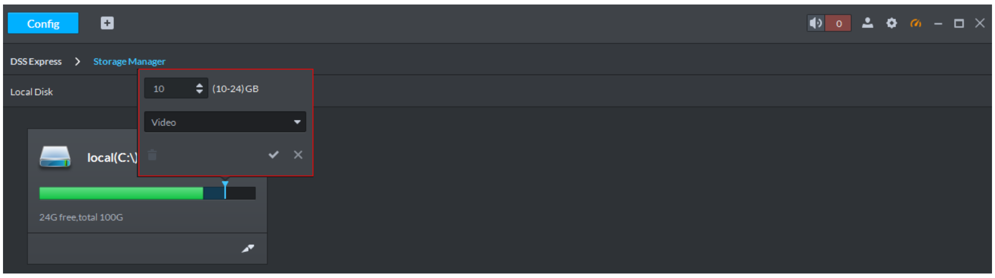
Figure 6-32 Storage manager



Step 2 Click ✎.

The system pops out the dialog of setting storage space size and type.

Figure 6-33 Create storage space



10 (10-24)GB

Video

Step 3 Set storage space size, select storage space type and click ✓.

Platform exclusive storage space is created on the disk. The exclusive storage space is displayed in the red box.

- When your scheme is TPC—Express, you need to configure both face image and video storage. When your scheme is TPC—IVSS/NVR—Express, you only need to configure face image storage (Video storage is optional).
- The minimum storage space is 10GB.
- Storage space type includes video, general picture and ANPR picture. Video disk is used to store video, general picture is used to store all snapshots except ANPR pictures.
- One local disk can divide general pictures for once top, but it can also modify storage space of general pictures.
- If you want to delete the storage space, you can click the storage segment, and delete exclusive space setting according to system prompt.

Figure 6-34 Disk status change

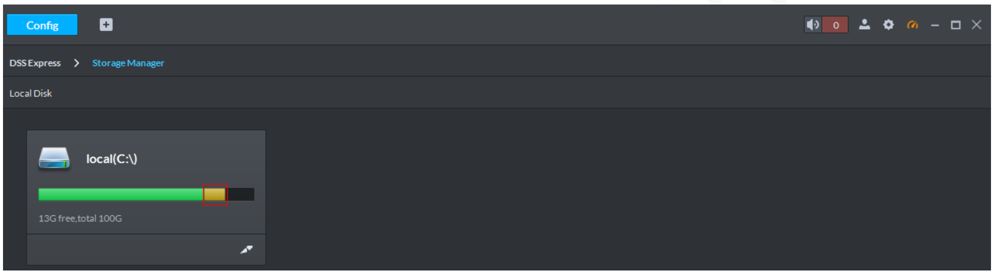
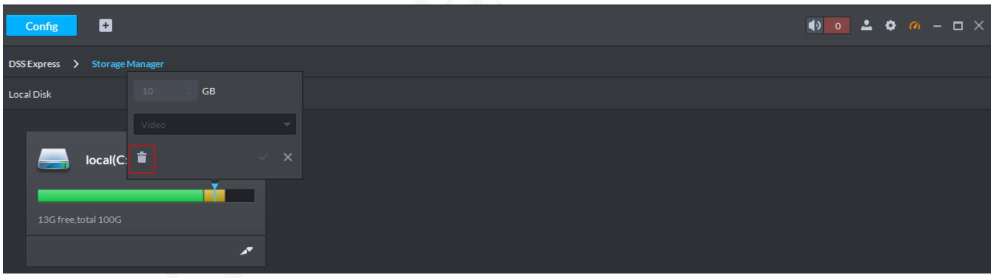


Figure 6-35 Delete exclusive storage space



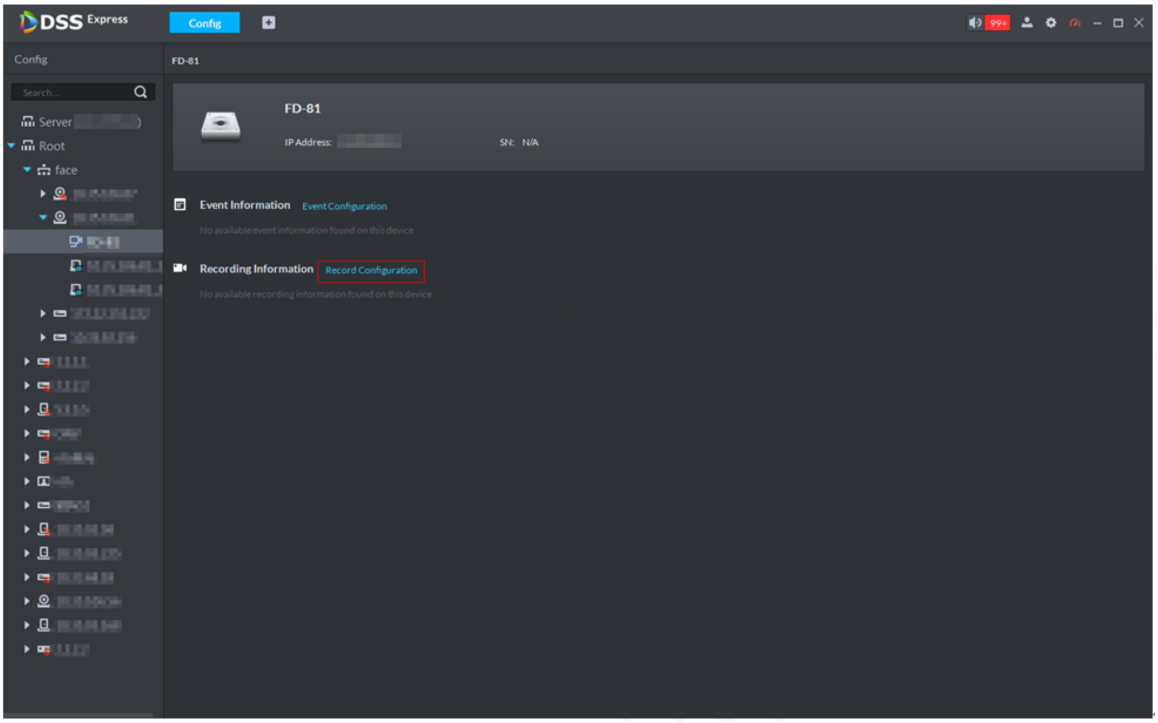
6.4.4 Configuring TPC Recording Plan

If IVSS/NVR is not included in your solution, you must configure recording plan on Express.

Step 1 Click **Config** on the client homepage.

Step 2 From the device tree on the left, select camera channel, click **Record Configuration**.

Figure 6-36 Enter record configuration interface



FD-81

IP Address: [redacted]   SN: N/A

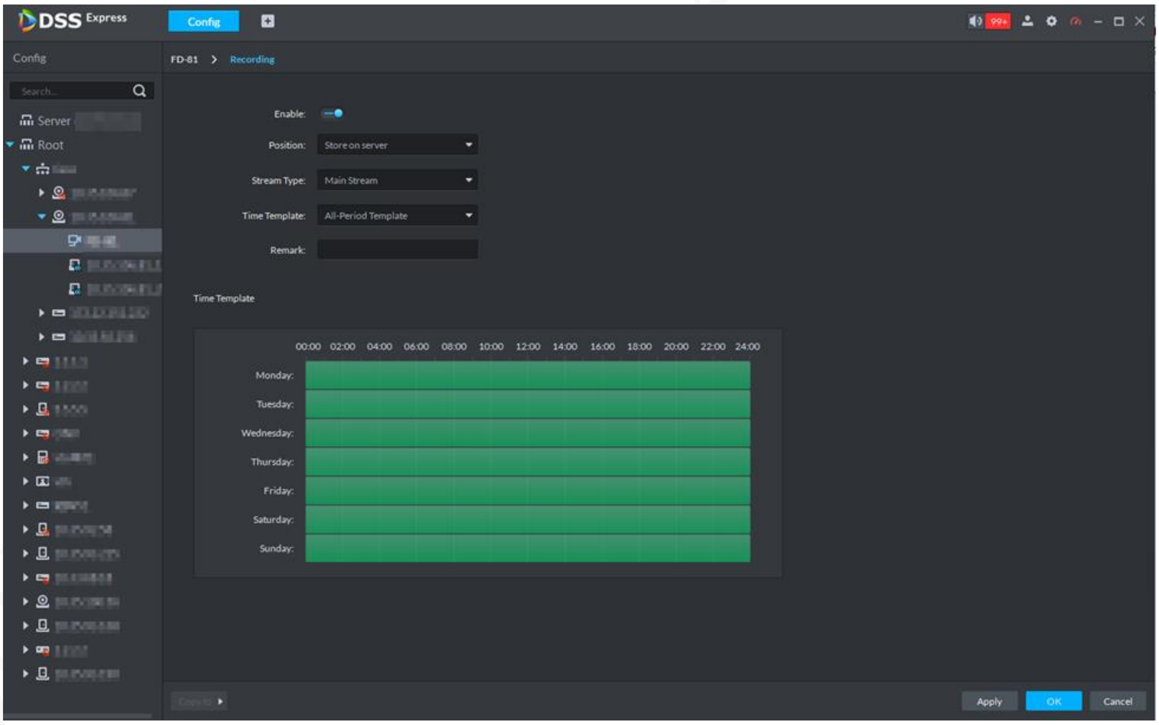
Event Information Event Configuration

No available event information found on this device

Recording Information Record Configuration

No available recording information found on this device

Figure 6-37 Record



Enable: ●

Position: Store on server

Stream Type: Main Stream

Time Template: All-Period Template

Remark:

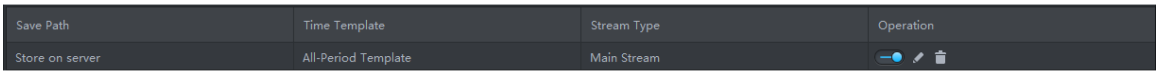
Step 3 Click ○.

The icon is switched to ●, enable record plan.

Step 4 Select Position, Stream Type and Time Template. Select Store on Server for Position.

Step 5 Click **OK**.

Figure 6-38 Record info



Save Path	Time Template	Stream Type	Operation
Store on server	All-Period Template	Main Stream	

6.4.1 Enabling Temperature, Blackbody or Mask Alarms

To be notified timely on Express when there is a temperature abnormal alarm, blackbody abnormal alarm or mask abnormal alarm, configure those alarm settings.

Step 1 Log in to Express client.

Step 2 Click **Config** on the client homepage.

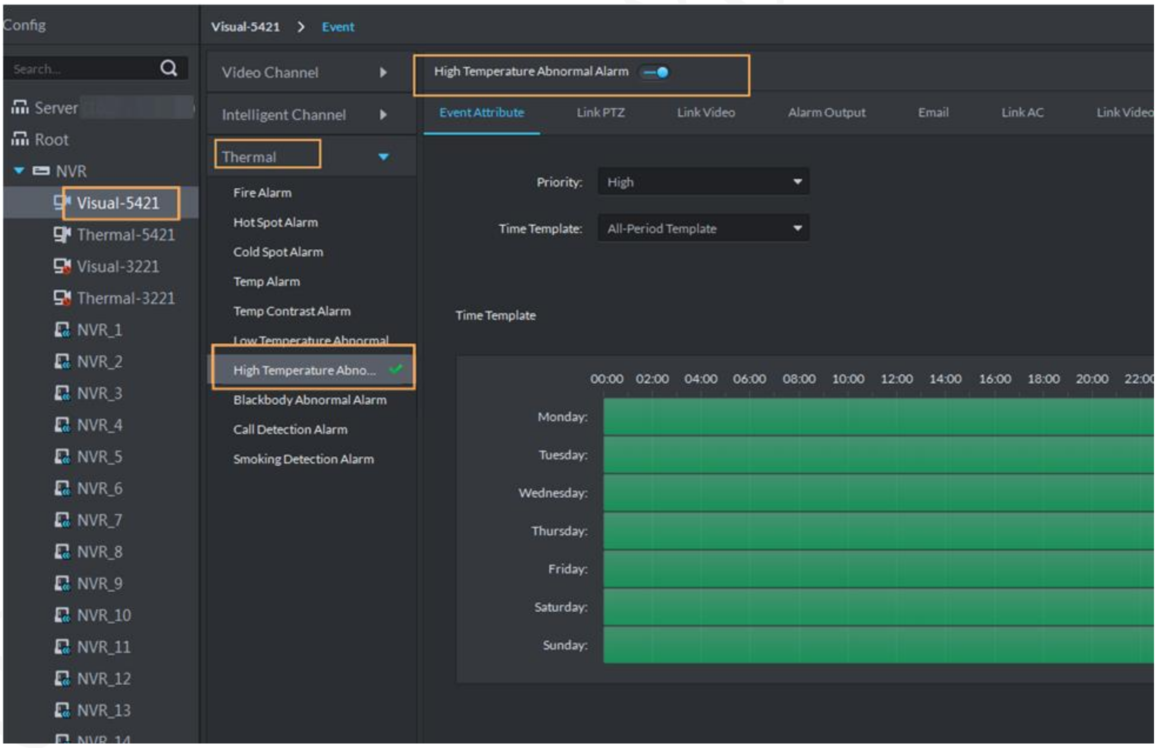
Step 3 Select the visual channel of the TPC from left device tree, and then click **Event Configuration**.

Step 4 Enable the alarm.

- Temperature abnormal alarm

  Click the **Thermal** tab, select the **High Temperature Abnormal Alarm** or **Low Temperature Abnormal Alarm**, and then click .

Figure 6-39 enable temperature abnormal alarm



Priority: High

Time Template: All-Period Template

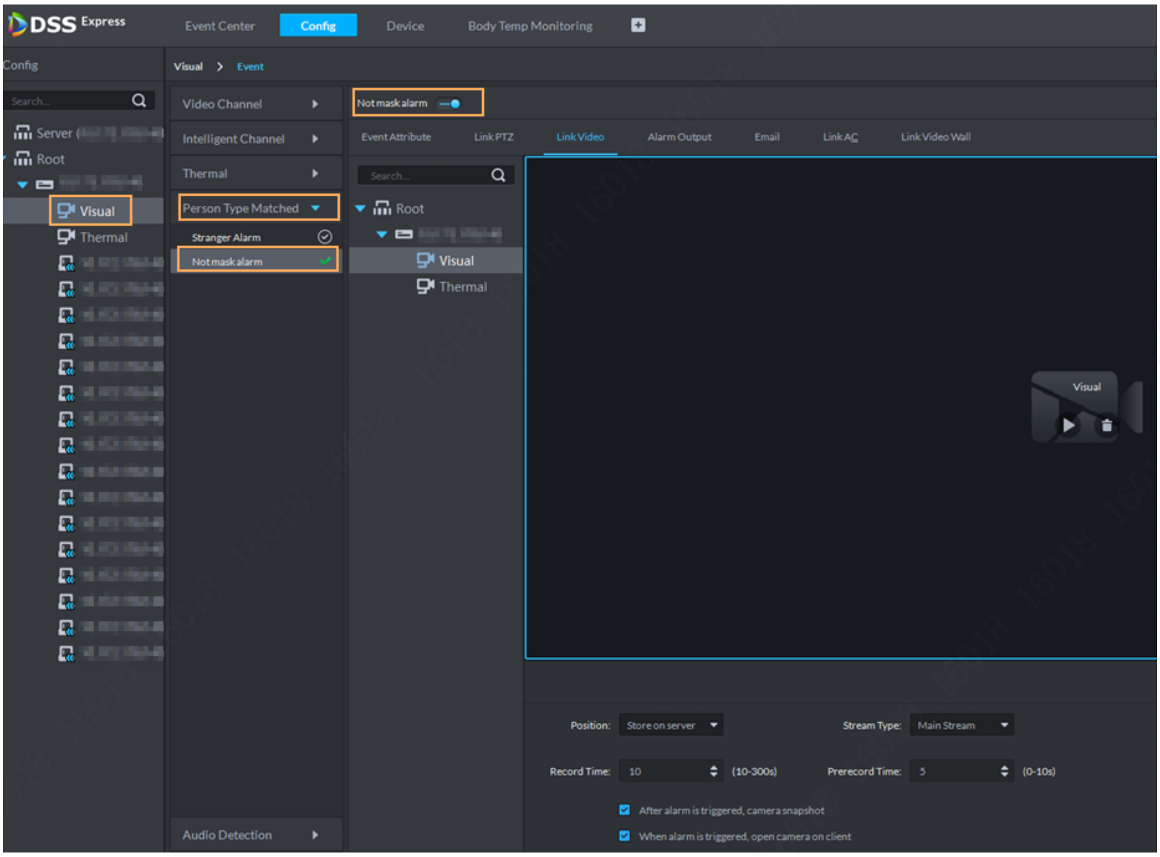
- Blackbody abnormal alarm

  Click the **Thermal** tab, select the **Blackbody Abnormal Alarm**, and then click .

- Mask abnormal alarm

  Click the **Person Type Matched** tab, select the **Not mask alarm**, and then click .

Figure 6-40 enable mask abnormal alarm



Position: Store on server

Stream Type: Main Stream

Record Time: 10 (10-300s)

Prerecord Time: 5 (0-10s)

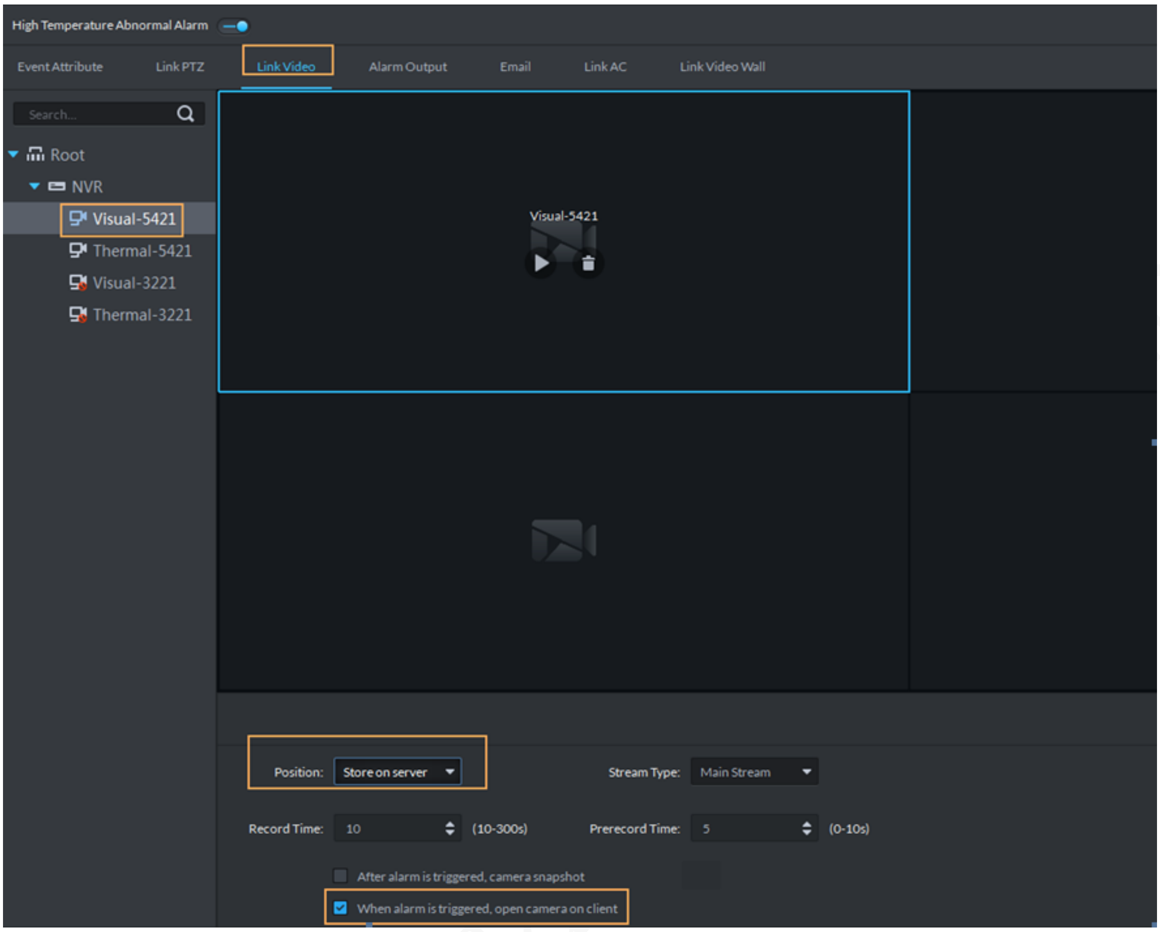
☑ After alarm is triggered, camera snapshot

☑ When alarm is triggered, open camera on client

Step 5 Set alarm priority and effective period.

1) Click the **Event Attribute** tab.
2) Select priority.
3) Select time template, you need to configure again if default time template fails to meet requirement.
4) Click the **Link Video** tab, select the visual channel of the TPC, select a window, and then drag the selected channel to the window.

Figure 6-41 Link video



Position: Store on server

Stream Type: Main Stream

Record Time: 10 (10-300s)

Prerecord Time: 5 (0-10s)

□ After alarm is triggered, camera snapshot

☑ When alarm is triggered, open camera on client

5) Set parameters.

Table 6-8 Link video parameter

Parameter	Description
Storage Position	Set storage position of videos and snapshots. Support storing on the server.
Stream Type	Select stream type for alarm video. Main stream has higher quality than sub stream, but consumes more storage and bandwidth than sub stream.
Record Time	Set time of linking record after alarm event is triggered.
Prerecord Time	Set prerecord duration. A pre-record is started seconds or minutes (as configured) before the event video.
After alarm is triggered, camera snapshot	Link corresponding camera snapshot after alarm event is triggered.
When alarm is triggered, open camera on client	After alarm output is triggered, you can open camera's real-time video on client.

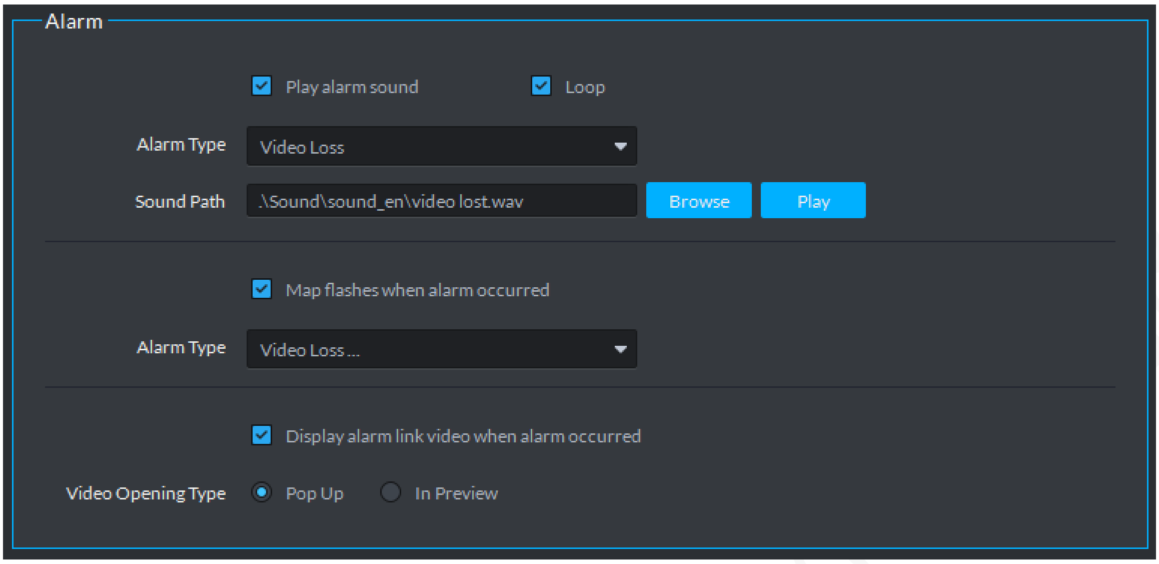
Step 6 Click **OK** and complete setting.

Step 7 Click ⚙ at upper-right corner of client interface.

The system displays **Local Config** interface.

Step 8 Click **Alarm** tab, set client alarm type.

Figure 6-42 Alarm



Alarm

☑ Play alarm sound ☑ Loop

Alarm Type: Video Loss

Sound Path: .\Sound\sound_en\video lost.wav

☑ Map flashes when alarm occurred

Alarm Type: Video Loss ...

☑ Display alarm link video when alarm occurred

Video Opening Type: ● Pop Up ○ In Preview

Step 9 Select the **Display alarm link video when alarm occurred** check box. System automatically opens linkage video when an alarm occurs.

Step 10 Select the **Pop Up** check box. System automatically opens linked video in a pop-up window when an alarm occurs.

6.5 Configuring DMSS

Skip this chapter if you do not have DMSS in your product combination.

6.5.1 Adding TPC to DMSS

You can add initialized devices through scanning device QR code, manually enter device SN, entering IP/domain, or searching online devices. This section takes adding TPC as an example.

6.5.1.1 Adding by SN/QR Code

You can add device by scanning device QR code or manually entering device SN.

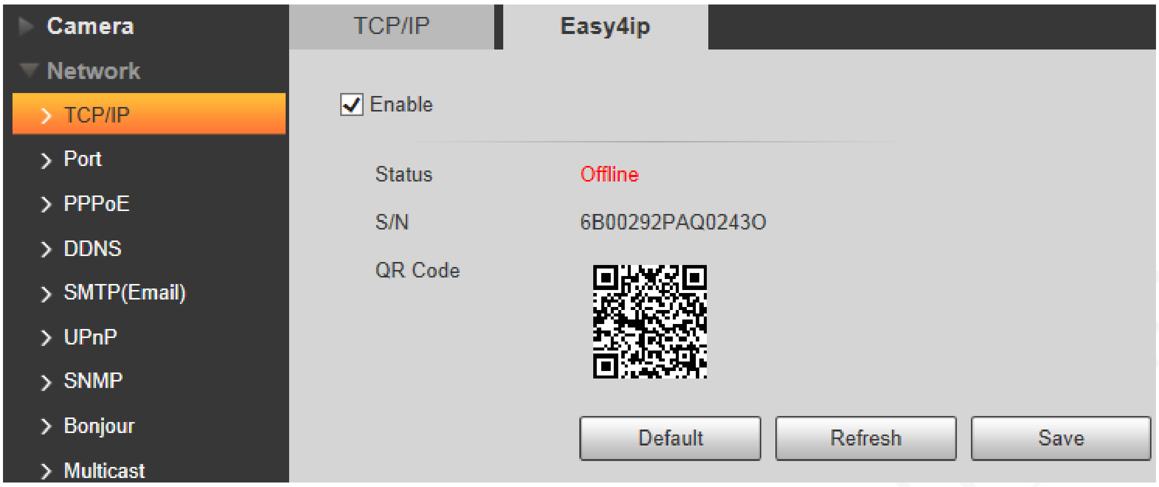
Step 1 On the **Home** interface, tap ⊕, and then select **SN/Scan**.

Step 2 Scan device QR code, or manually enter device SN, and then the system will identify the device type automatically. If the device type cannot be automatically identified by the system, you need to select the device type.

If you scan QR code to add TPC, follow the following steps.

1) On TPC web interface, select **Setting > Network > TCP/IP > Easy4ip**.
2) Select **Enable** and click **Save**.
3) Scan the QR code.

Figure 6-43 Scanning the QR code



☑ Enable

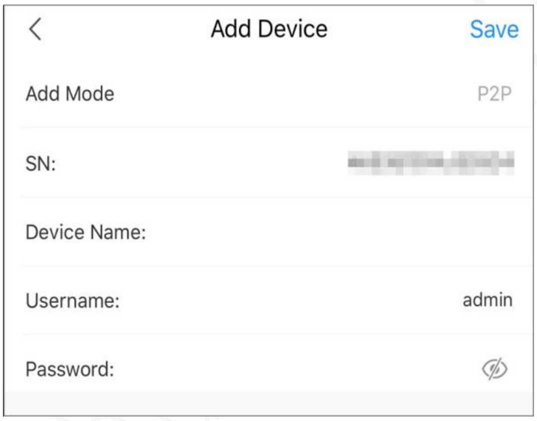
Status Offline

S/N 6B00292PAQ0243O

QR Code

Step 3 Enter device name, device password, and save settings.

Figure 6-44 Add initialized device (SN/scan)



Add Mode P2P

SN: [redacted]

Device Name:

Username: admin

Password:

6.5.1.2 Adding by IP/Domain

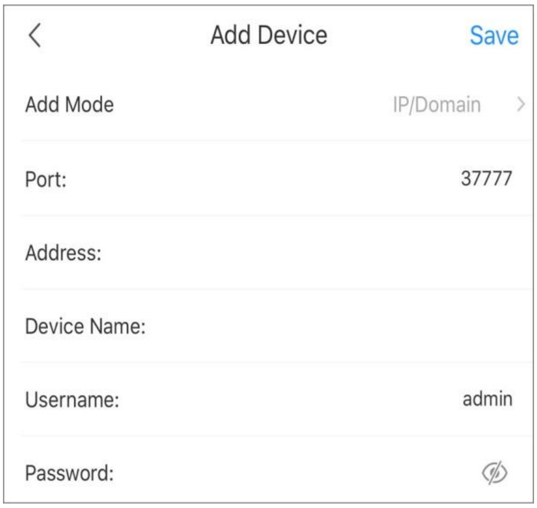
You can add devices by entering IP of the device or specific domain. This section takes entering device IP as an example.

Step 1 On the **Home** interface, tap ⊕, and then select **IP/Domain**.

Step 2 Select the device type.

Step 3 Enter information as needed, and then save settings.

Figure 6-45 Add initialized device (IP/domain)

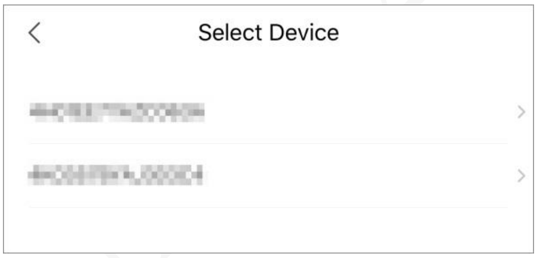

Add Device
Save
Add Mode IP/Domain
Port: 37777
Address:
Device Name:
Username: admin
Password:

6.5.1.3 Adding by Search

You can search online devices and add them.

Step 1 Tap ⊕ at the upper-right corner, and then select **Search online**.

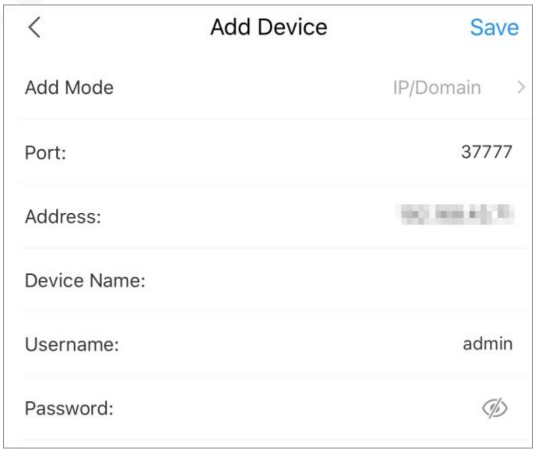
Figure 6-46 Select device SN


Select Device
[redacted]
[redacted]

Step 2 Tap the device SN as needed.

Step 3 Select the device type.

Figure 6-47 Add initialized device (search online)


Add Device
Save
Add Mode IP/Domain
Port: 37777
Address: [redacted]
Device Name:
Username: admin
Password:

Step 4 Enter information as needed, and then save settings.

6.5.2 Configuring TPC Video/Image Storage

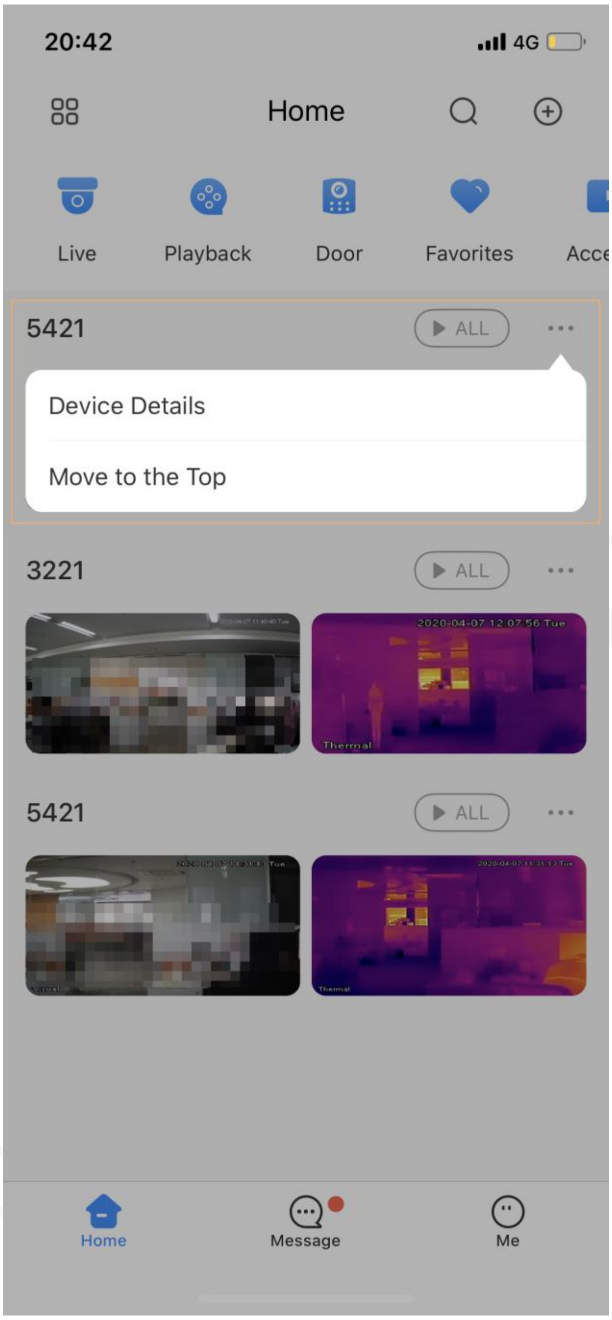
For TPC–IVSS/NVR–DMSS, store video/image on IVSS or NVR. For TPC–Face Recognition Terminal–DMSS or TPC–DMSS, store video/image on SD card or DMSS cloud (you need to purchase SD card or DMSS cloud separately).

6.5.3 Subscribing Elevated Temperature Alarm

Subscribing elevated temperature alarm on DMSS to help you receive alarm information and take actions in time.

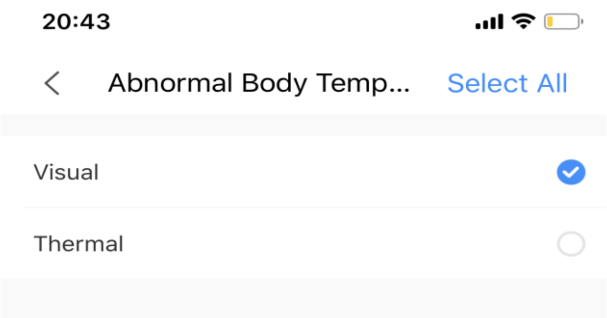
Step 1 On DMSS main interface, select a TPC and click ⋯. Then click **Device Details**.

Figure 6-48 Selecting a TPC



Step 2 Select **Alarm Subscription > Abnormal Body Temperature** and select a channel.

Figure 6-49 Selecting channel



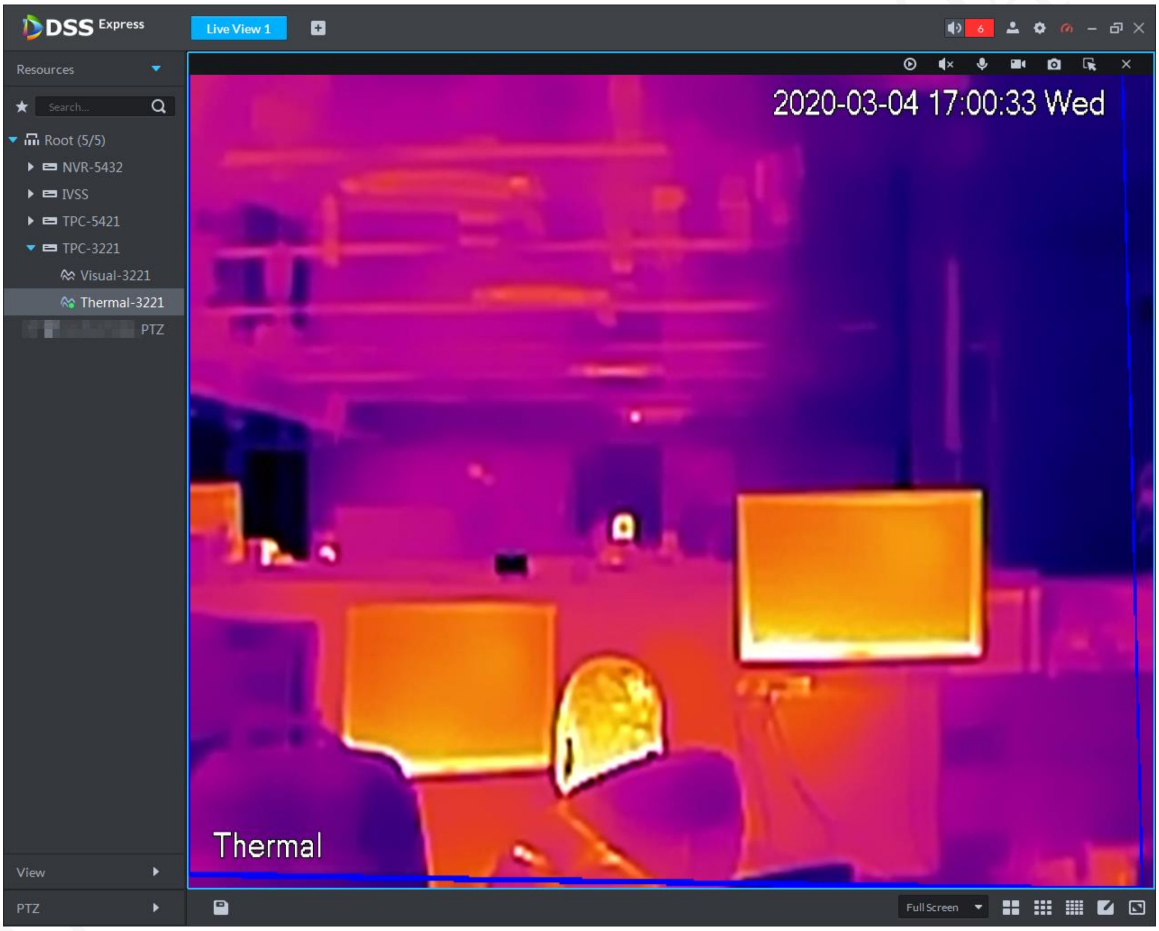
6.6 Commissioning

6.6.1 Commissioning Express

6.6.1.1 Viewing Live View

Select the TPC camera from device list on the **Live View** interface, double-click or drag to the video window. The system plays real-time video.

Figure 6-50 Live view



6.6.1.2 Temperature, Blackbody or Mask Alarms

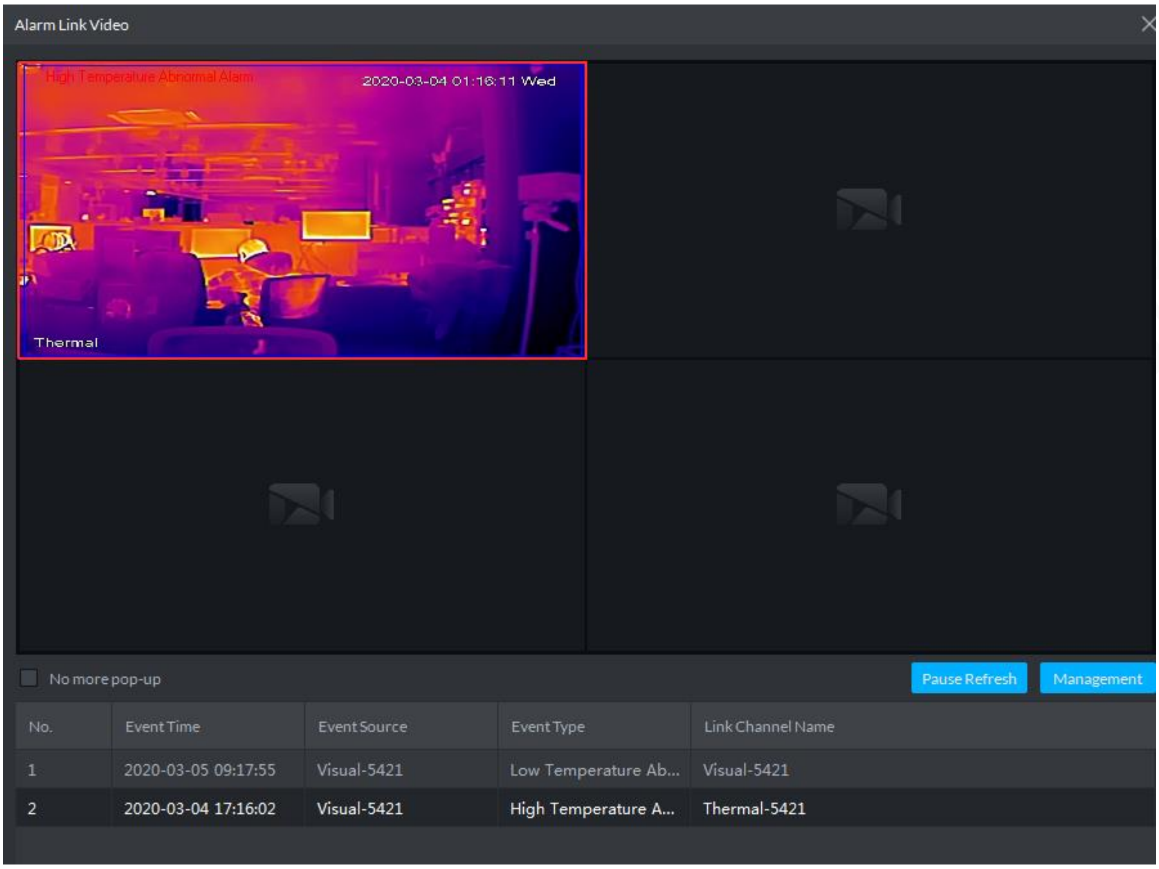
- Human body temperature alarm

  Trigger a human body temperature alarm, and then check:

  ◇ Whether the sound and light warnings are triggered on the camera.

  ◇ Whether the Express displays the alarm correctly in a pop-up window.

Figure 6-51 High temperature alarm



□ No more pop-up

No.	Event Time	Event Source	Event Type	Link Channel Name
1	2020-03-05 09:17:55	Visual-5421	Low Temperature Ab...	Visual-5421
2	2020-03-04 17:16:02	Visual-5421	High Temperature A...	Thermal-5421

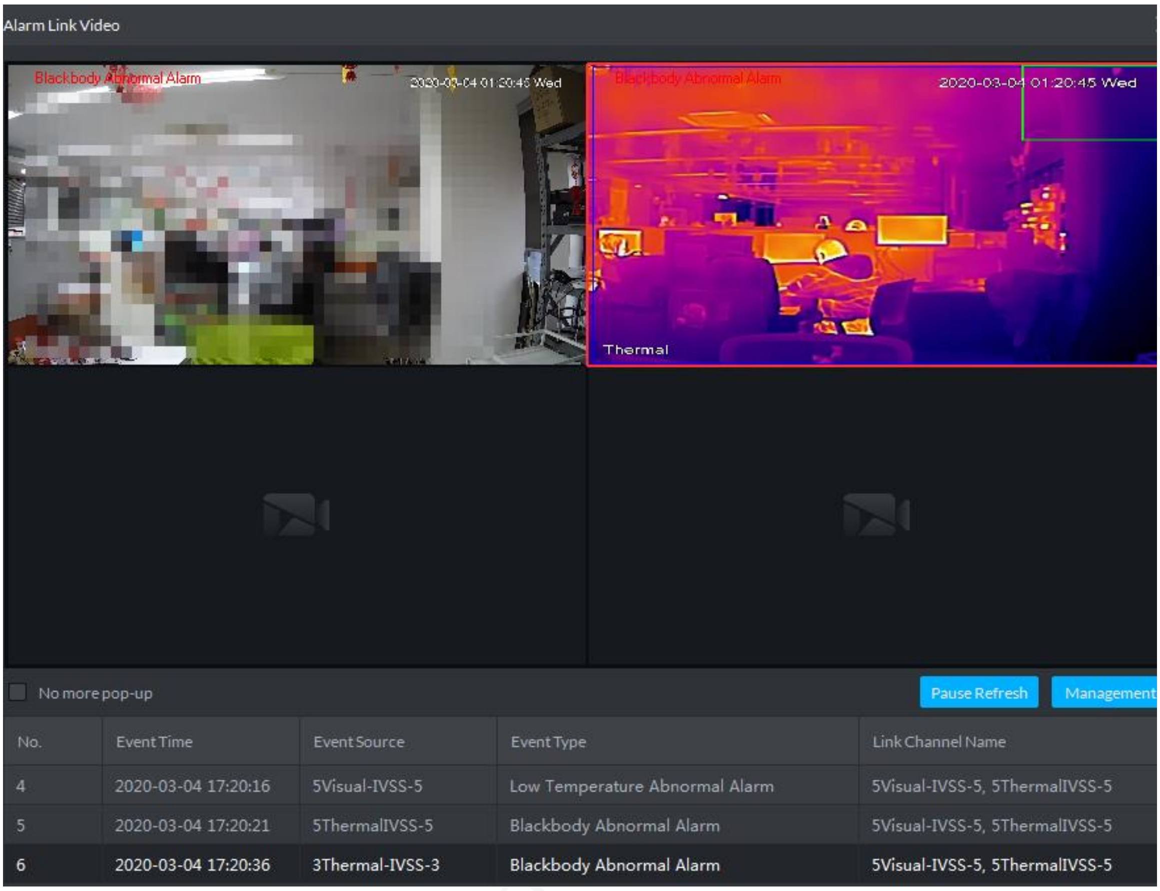
- Black body abnormality alarm

  Trigger a blackbody abnormal alarm, and then check:

  ◇ Whether the sound and light warnings are triggered on the camera.

  ◇ Whether the Express displays the alarm correctly in a pop-up window.

Figure 6-52 Blackbody abnormality alarm



No.	Event Time	Event Source	Event Type	Link Channel Name
4	2020-03-04 17:20:16	5Visual-IVSS-5	Low Temperature Abnormal Alarm	5Visual-IVSS-5, 5ThermalIVSS-5
5	2020-03-04 17:20:21	5ThermalIVSS-5	Blackbody Abnormal Alarm	5Visual-IVSS-5, 5ThermalIVSS-5
6	2020-03-04 17:20:36	3Thermal-IVSS-3	Blackbody Abnormal Alarm	5Visual-IVSS-5, 5ThermalIVSS-5

- Mask abnormal alarm

  Trigger a mask abnormal alarm, and then check:

  ◇ Whether the sound and light warnings are triggered on the camera.

  ◇ Whether the Express displays the alarm correctly in the pop-up window.

6.6.2 Commissioning DMSS

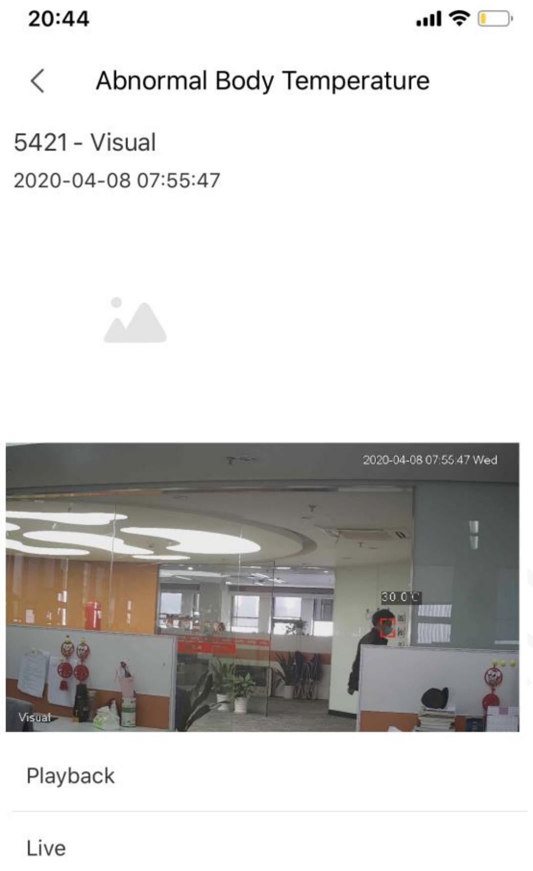
6.6.2.1 Viewing Live View

Select the TPC camera from device list on the main interface, click the device image. The system plays real-time video.

6.6.2.2 Elevated Body Temperature Alarm

Trigger a human body temperature alarm, and then check whether the DMSS displays the alarm correctly.

Figure 6-53 Body temperature alarm



20:44

Abnormal Body Temperature

5421 - Visual

2020-04-08 07:55:47

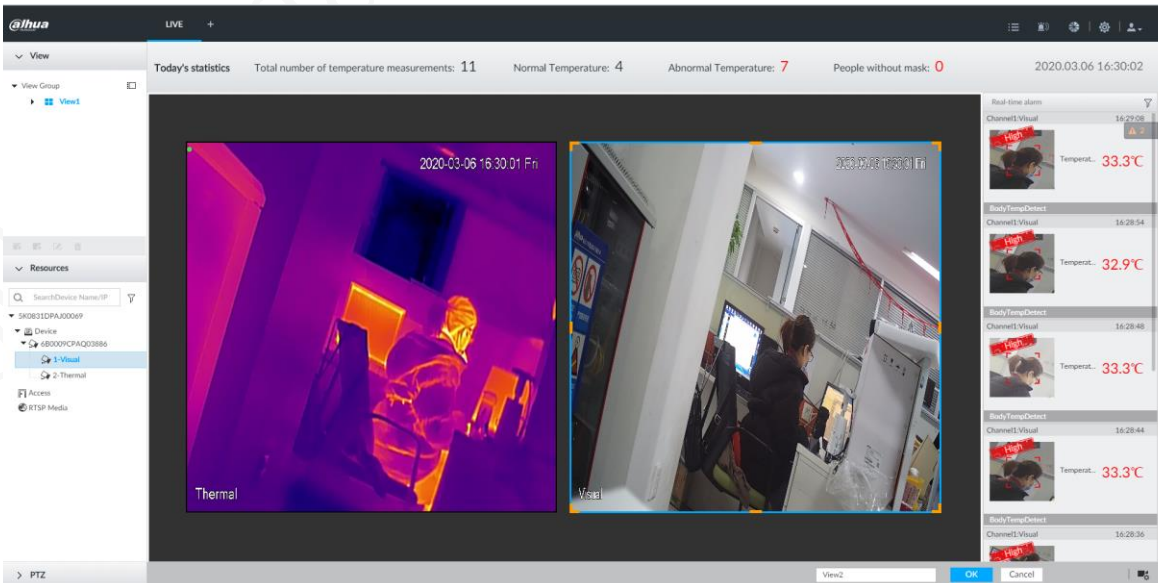
Playback

Live

6.6.3 Viewing Live View on IVSS

Select the TPC camera from device list on the **Live View** interface, double-click or drag to the video window. The system plays real-time video and detection results..

Figure 6-54 Live view

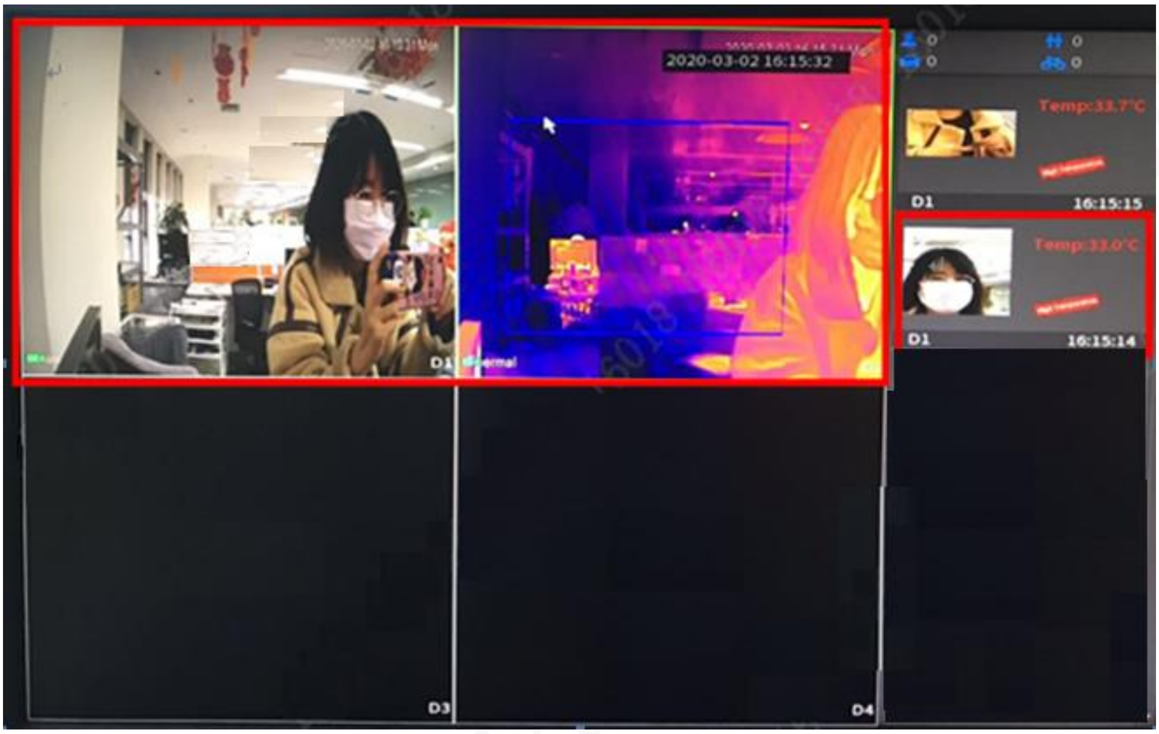


Today's statistics Total number of temperature measurements: 11 Normal Temperature: 4 Abnormal Temperature: 7 People without mask: 0 2020.03.06 16:30:02

6.6.4 Viewing Live View on NVR

Select the TPC camera from device list on the **Live View** interface, double-click or drag to the video window. The system plays real-time video and detection results.

Figure 6-55 Live view



Appendix 1 Cybersecurity Recommendations

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

Mandatory actions to be taken for basic equipment network security:

1. **Use Strong Passwords**

   Please refer to the following suggestions to set passwords:

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

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

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

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

1. **Physical Protection**

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

2. **Change Passwords Regularly**

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

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

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

4. **Enable Account Lock**

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

5. **Change Default HTTP and Other Service Ports**
   We suggest you to change default HTTP and other service ports into any set of numbers between 1024~65535, reducing the risk of outsiders being able to guess which ports you are using.
6. **Enable HTTPS**
   We suggest you to enable HTTPS, so that you visit Web service through a secure communication channel.
7. **Enable Whitelist**
   We suggest you to enable whitelist function to prevent everyone, except those with specified IP addresses, from accessing the system. Therefore, please be sure to add your computer's IP address and the accompanying equipment's IP address to the whitelist.
8. **MAC Address Binding**
   We recommend you to bind the IP and MAC address of the gateway to the equipment, thus reducing the risk of ARP spoofing.
9. **Assign Accounts and Privileges Reasonably**
   According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.
10. **Disable Unnecessary Services and Choose Secure Modes**
    If not needed, it is recommended to turn off some services such as SNMP, SMTP, UPnP, etc., to reduce risks.
    If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:
    - SNMP: Choose SNMP v3, and set up strong encryption passwords and authentication passwords.
    - SMTP: Choose TLS to access mailbox server.
    - FTP: Choose SFTP, and set up strong passwords.
    - AP hotspot：Choose WPA2-PSK encryption mode, and set up strong passwords.
11. **Audio and Video Encrypted Transmission**
    If your audio and video data contents are very important or sensitive, we recommend that you use encrypted transmission function, to reduce the risk of audio and video data being stolen during transmission.
    Reminder: encrypted transmission will cause some loss in transmission efficiency.
12. **Secure Auditing**
    - Check online users: we suggest that you check online users regularly to see if the device is logged in without authorization.
    - Check equipment log: By viewing the logs, you can know the IP addresses that were used to log in to your devices and their key operations.
13. **Network Log**
    Due to the limited storage capacity of the equipment, the stored log is limited. If you need to save the log for a long time, it is recommended that you enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.
14. **Construct a Safe Network Environment**
    In order to better ensure the safety of equipment and reduce potential cyber risks, we recommend:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network.
- The network should be partitioned and isolated according to the actual network needs. If there are no communication requirements between two sub networks, it is suggested to use VLAN, network GAP and other technologies to partition the network, so as to achieve the network isolation effect.
- Establish the 802.1x access authentication system to reduce the risk of unauthorized access to private network.
- It is recommended that you enable your device's firewall or blacklist and whitelist feature to reduce the risk that your device might be attacked.

ENABLING A SAFER SOCIETY AND SMARTER LIVING