# Dahua Access Control Body Temperature Monitoring Solution

## Deployment Guide

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

V1.0.0

# 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. | May 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

**Foreword ........ I**

**Important Safeguards and Warnings ........ III**

**1 Overview ........ 1**

**2 Network Diagram ........ 2**

**3 Deployment Process ........ 5**

**4 Installation ........ 7**

4.1 Installing Express ........ 7

4.1.1 Installing Express Service ........ 7

4.1.2 Installing Express PC Client ........ 9

4.1.3 Logging in to Express ........ 12

4.1.4 Licensing Express ........ 12

4.2 Installing Face Recognition Terminal ........ 14

4.3 Installing DMSS ........ 15

**5 Getting Started ........ 16**

5.1 Initializing NVR ........ 16

5.1.1 Initializing NVR with ConfigTool ........ 16

5.1.2 Modifying IP Address ........ 17

5.1.3 Updating System ........ 18

5.2 Initializing Face Recognition Terminal ........ 22

5.2.1 Initializing Face Recognition Terminal with ACS ConfigTool ........ 22

5.2.2 Modifying IP Address ........ 24

5.2.3 Updating System ........ 25

**6 Configuration and Commissioning ........ 28**

6.1 Configuring Face Recognition Terminal ........ 28

6.1.1 Configuring Unlock Mode ........ 28

6.1.2 Creating Face Database ........ 29

6.1.3 Configuring Face Recognition Parameters ........ 32

6.1.4 Commissioning ........ 35

6.2 Configuring NVR ........ 38

6.2.1 Adding Face Recognition Terminal to NVR ........ 38

6.2.2 Enabling Temperature and Mask Monitoring ........ 41

6.2.3 (Optional) Enabling Fahrenheit ........ 42

6.2.4 Commissioning ........ 42

6.3 Configuring Express ........ 43

6.3.1 Configuring Storage Space on Express ........ 43

6.3.2 Configuring Video Recording Plan on Express ........ 47

6.3.3 Adding Face Recognition Terminal to Express ........ 44

6.3.4 Modifying Channel Number and Features ........ 47

6.3.5 Configuring People Information ........ 49

6.3.6 Configuring Door Unlock Method ........ 54

6.3.7 Configuring Temperature and Mask Alarms ........ 56

6.3.8 Commissioning ........ 57

6.4 Configuring DMSS ........ 59
6.4.1 Adding Face Recognition Terminal to DMSS ........ 59
6.4.2 Configuring Video/Image Storage ........ 61
6.4.3 Subscribing Alarms ........ 61
6.4.4 Commissioning ........ 62
**Appendix 1 Cybersecurity Recommendations ........ 64**

# 1 Overview

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

In this solution, face recognition terminals measure human body temperature and recognize faces (hereinafter referred to as TPC), and then upload the measurement results attached with face and identification information to NVR, or the central platform Express, or mobile App DMSS, so as to notify inspectors and provide evidences.

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

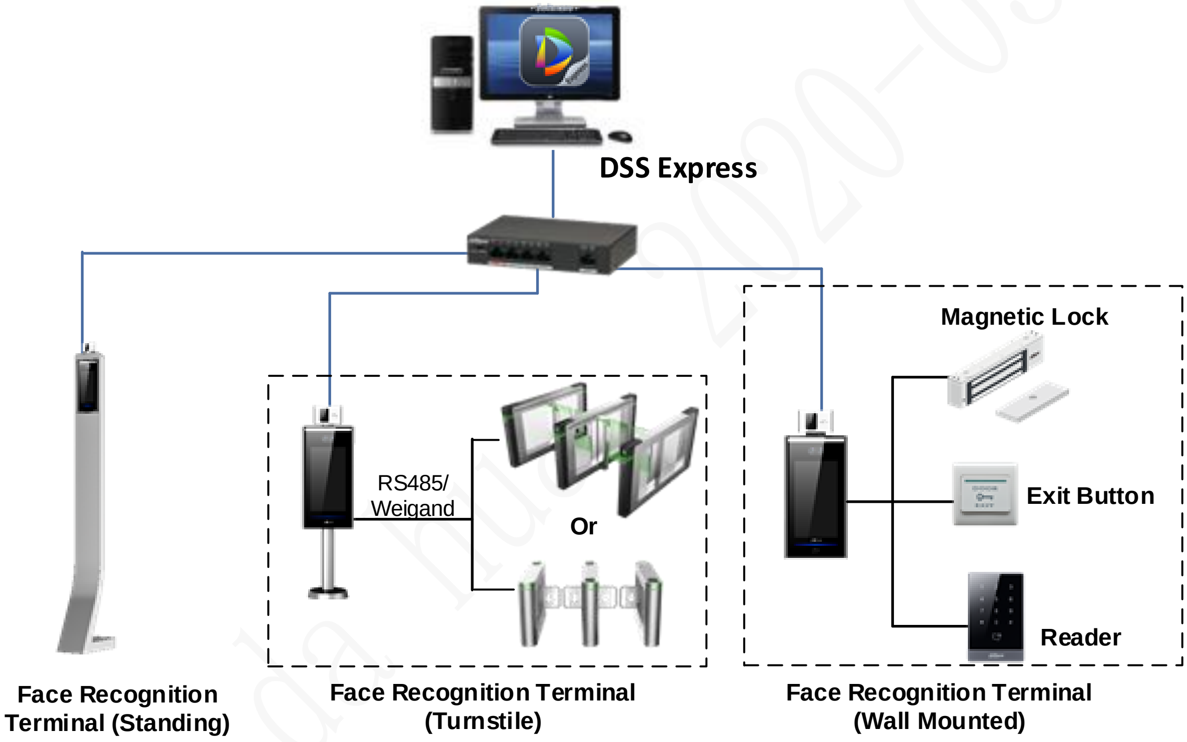
There are three combinations of products. See the topologies below.

- Face Recognition Terminal – Express

  Face recognition terminal and Express server are connected to the network switch. The turnstile connects to the terminal through RS–485 or Weigand. Images and videos are stored in the disks of Express server.

  Face recognition terminal recognizes faces, measures face temperature, and then uploads the results to Express. Express receives and displays live videos, images and alarms from the terminal, and centrally manages the system.

Figure 2-1 Face Recognition Terminal–Express

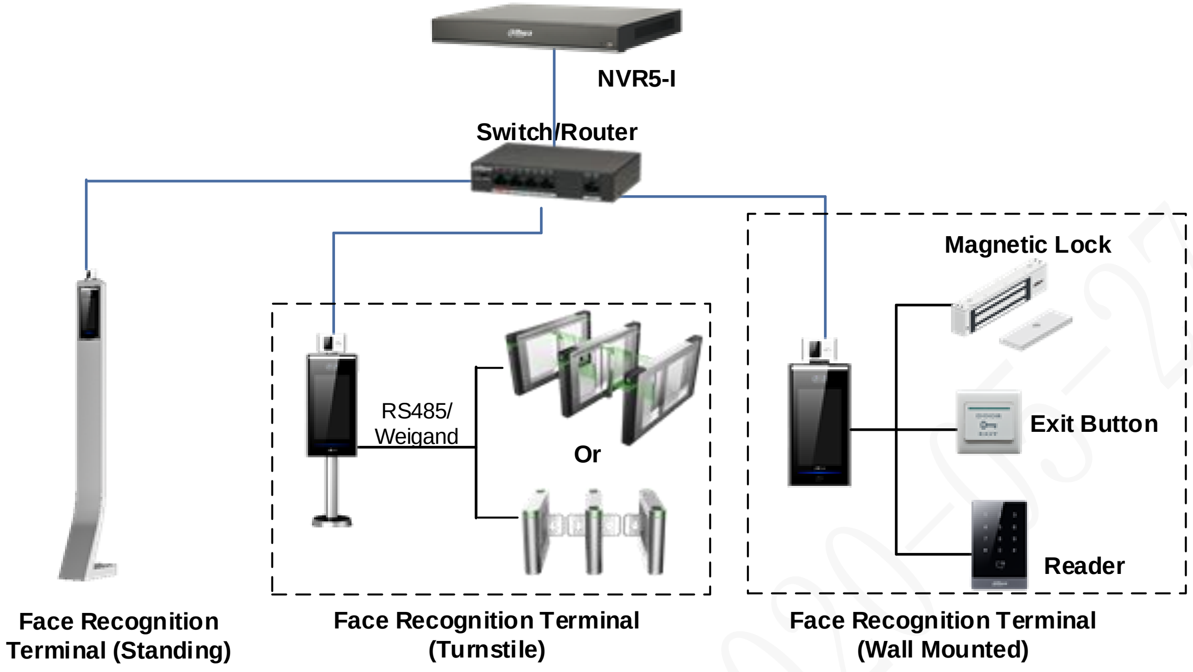

DSS Express
Magnetic Lock
RS485/
Weigand
Or
Exit Button
Reader
Face Recognition Terminal (Standing)
Face Recognition Terminal (Turnstile)
Face Recognition Terminal (Wall Mounted)

- Face Recognition Terminal – NVR

  Face recognition terminal and NVR are connected to the network switch. The turnstile connects to the terminal through RS–485 or Weigand.

  Face recognition terminal recognizes faces, measures face temperature, and then uploads the results to NVR. NVR receives and displays live videos, images and alarms from the terminal.

Figure 2-2 Face Recognition Terminal–NVR

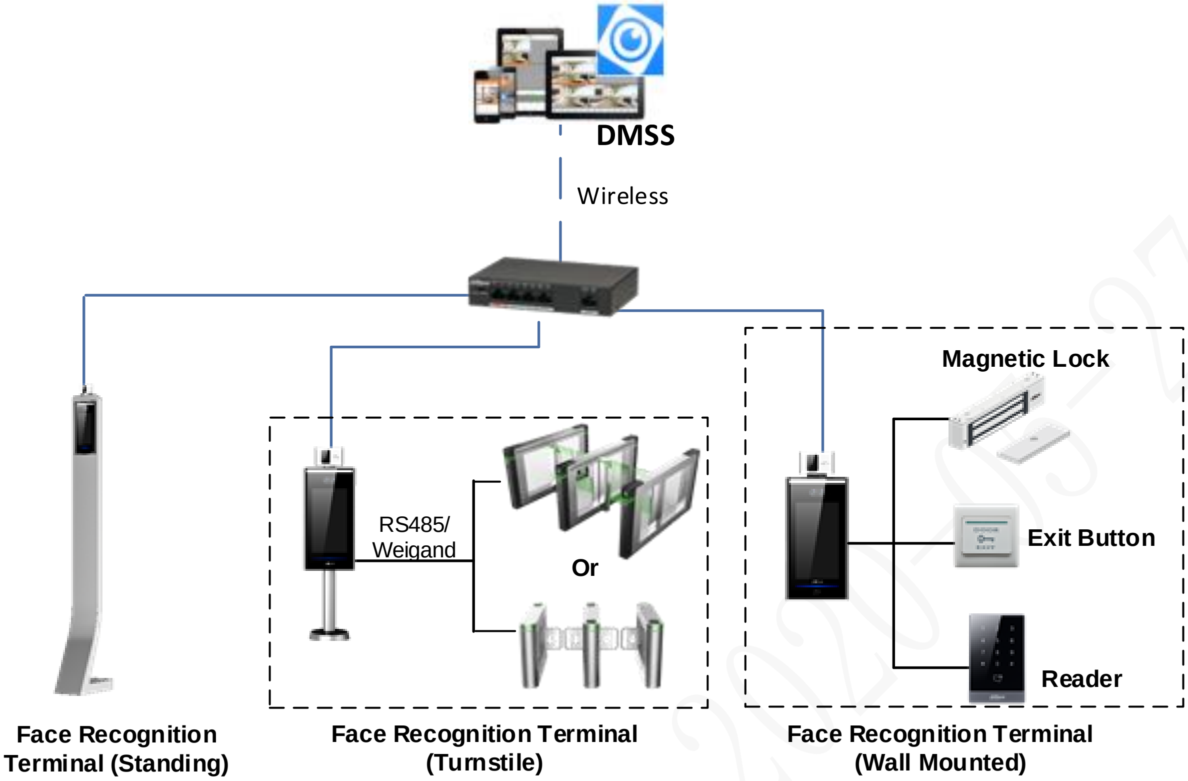

NVR5-I
Switch/Router
Magnetic Lock
RS485/
Weigand
Or
Exit Button
Reader
Face Recognition Terminal (Standing)
Face Recognition Terminal (Turnstile)
Face Recognition Terminal (Wall Mounted)

- Face Recognition Terminal – DMSS

  Face recognition terminal is connected to the network switch. DMSS is installed on the mobile devices such as phone. The turnstile connects to the terminal through RS–485 or Weigand.

  Face recognition terminal recognizes faces, measures face temperature, and then uploads the results to DMSS. DMSS receives and displays live videos, images and alarms from the terminal.

Figure 2-3 Face Recognition Terminal–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

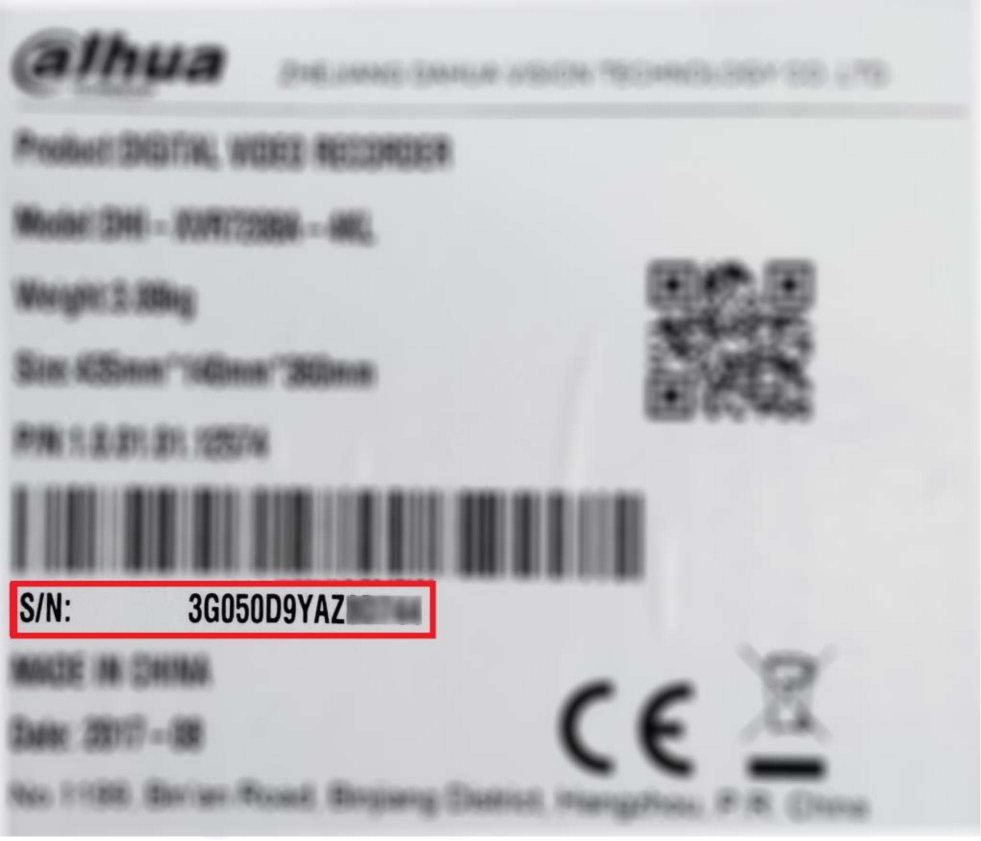
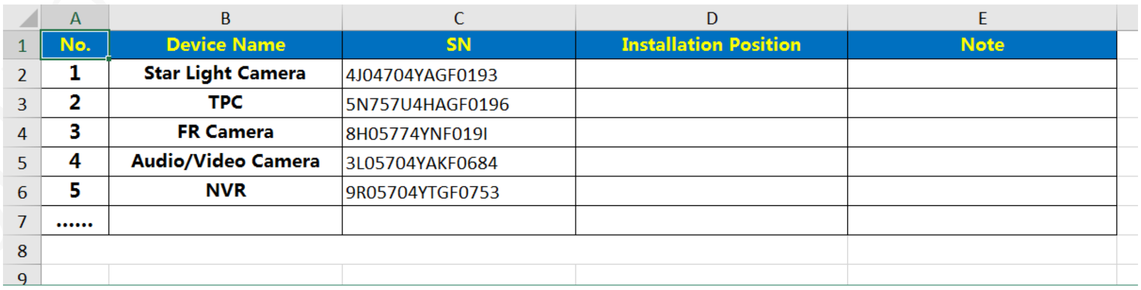


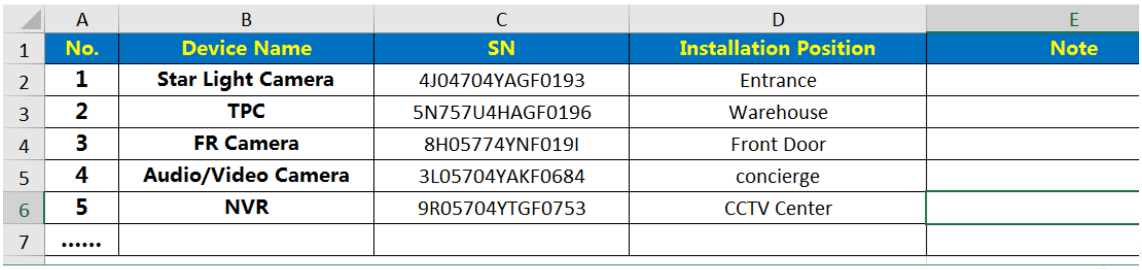
Figure 3-2 Record SN numbers



| 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.

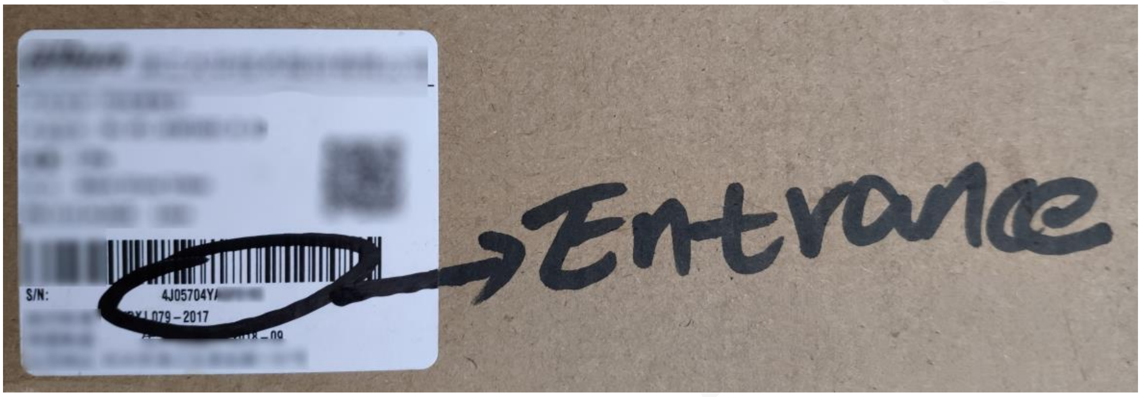
Figure 3-3 Match installation position



|   | A | B | C | D | E |
|---|---|---|---|---|---|
| 1 | No. | Device Name | SN | Installation Position | Note |
| 2 | 1 | Star Light Camera | 4J04704YAGF0193 | Entrance |  |
| 3 | 2 | TPC | 5N757U4HAGF0196 | Warehouse |  |
| 4 | 3 | FR Camera | 8H05774YNF019I | Front Door |  |
| 5 | 4 | Audio/Video Camera | 3L05704YAKF0684 | concierge |  |
| 6 | 5 | NVR | 9R05704YTGF0753 | CCTV Center |  |
| 7 | …… |  |  |  |  |

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."

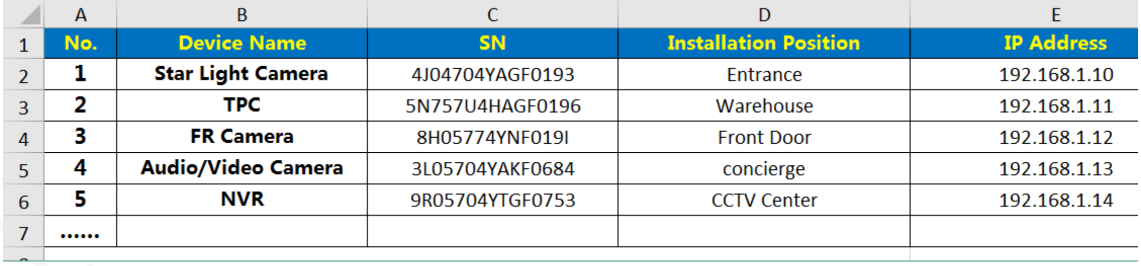
Figure 3-4 Mark installation position



Step 5 Make sure that all the devices are properly connected, and then power up all the devices. 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



|   | A | B | C | D | E |
|---|---|---|---|---|---|
| 1 | No. | Device Name | SN | Installation Position | IP Address |
| 2 | 1 | Star Light Camera | 4J04704YAGF0193 | Entrance | 192.168.1.10 |
| 3 | 2 | TPC | 5N757U4HAGF0196 | Warehouse | 192.168.1.11 |
| 4 | 3 | FR Camera | 8H05774YNF019I | Front Door | 192.168.1.12 |
| 5 | 4 | Audio/Video Camera | 3L05704YAKF0684 | concierge | 192.168.1.13 |
| 6 | 5 | NVR | 9R05704YTGF0753 | CCTV Center | 192.168.1.14 |
| 7 | …… |  |  |  |  |

Step 7 Configure devices and carry out commissioning. See "6 Configuration and Commissioning."

# 4 Installation

Follow the product manuals to install and connect the products. Pay attention to the following considerations.

## 4.1 Installing Express

### 4.1.1 Installing Express Service

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

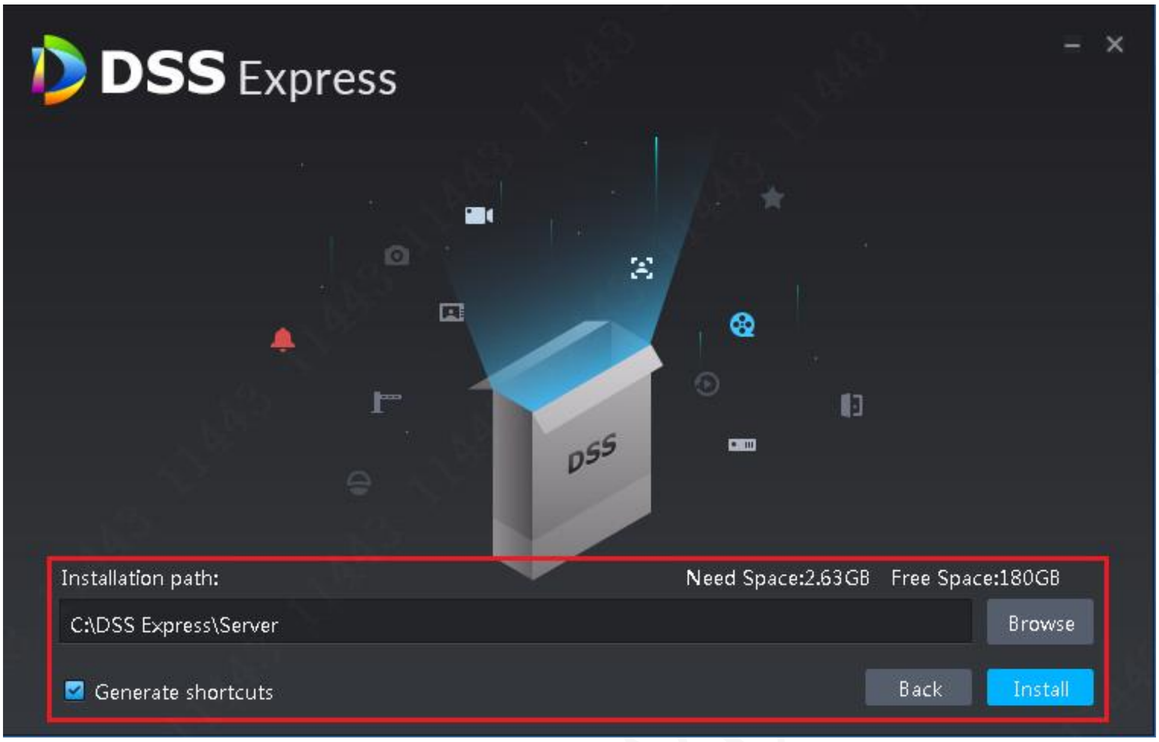
Table 4-1 Server configuration requirement

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

Step 1 Double-click installer.

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

Figure 4-1 Select installation path



C:\DSS Express\Server

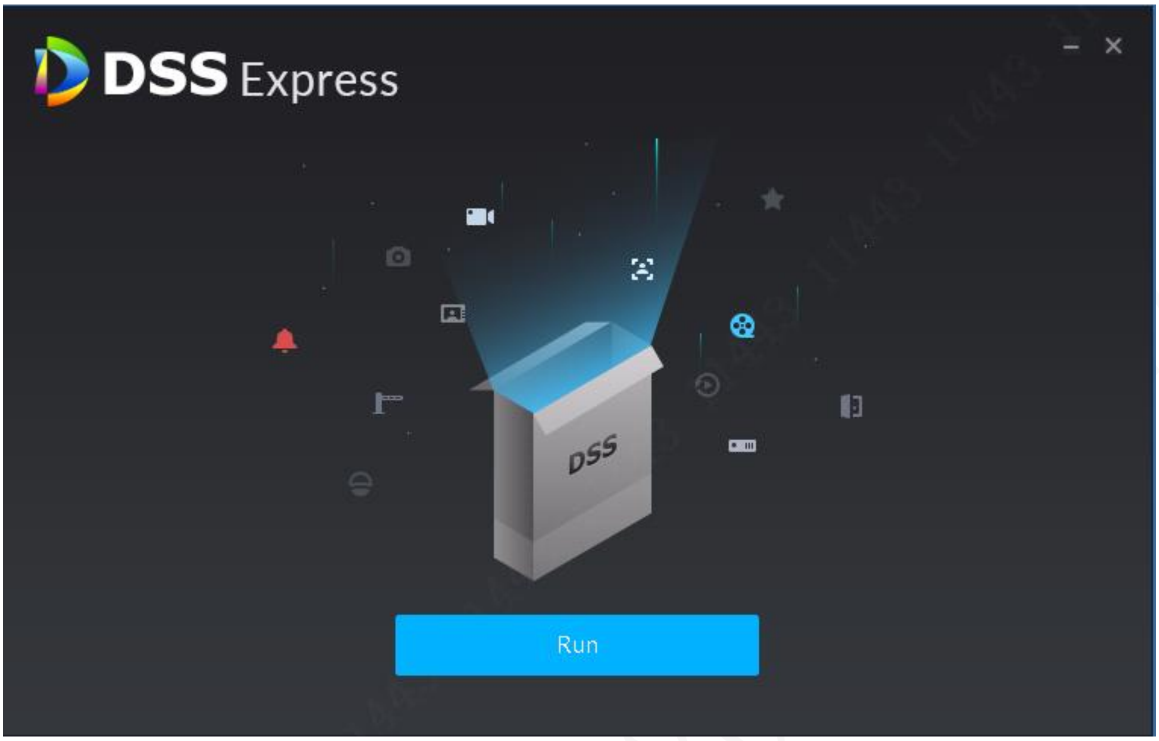
☑ Generate shortcuts

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

The system displays installation progress, the whole installation needs 5-10 minutes. See Figure 4-2 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 4-2 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**.

### 4.1.2 Installing Express PC Client

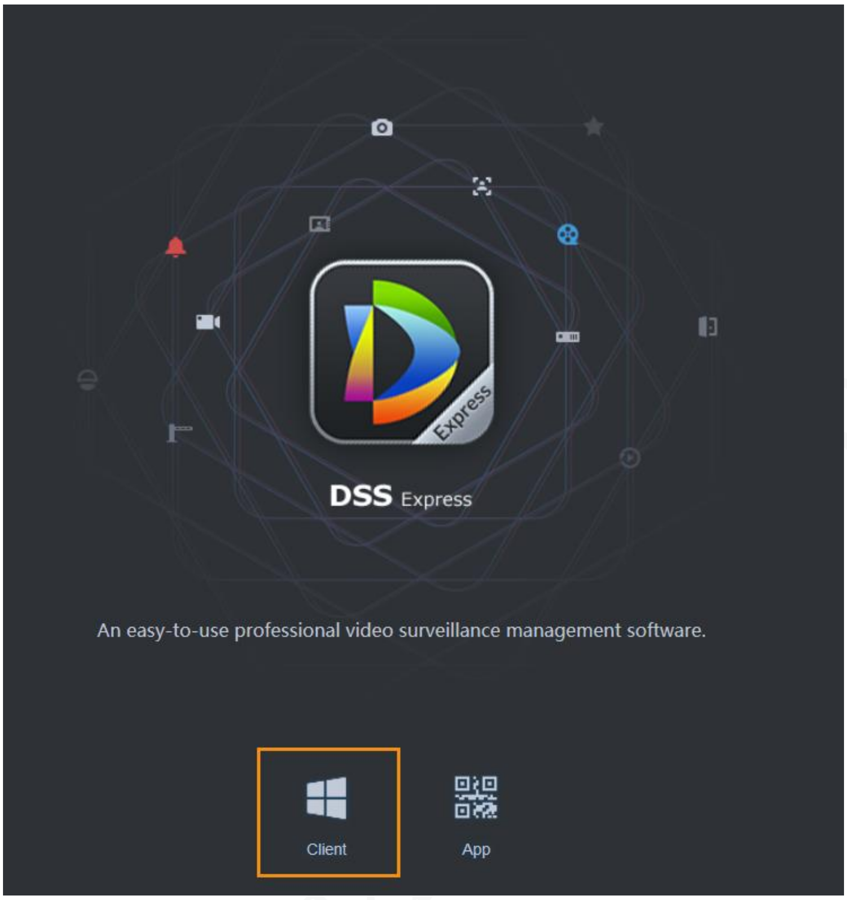
Follow this table to prepare a PC for installing Express client.

Table 4-2 Configuration requirement

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

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

Figure 4-3 Download client



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

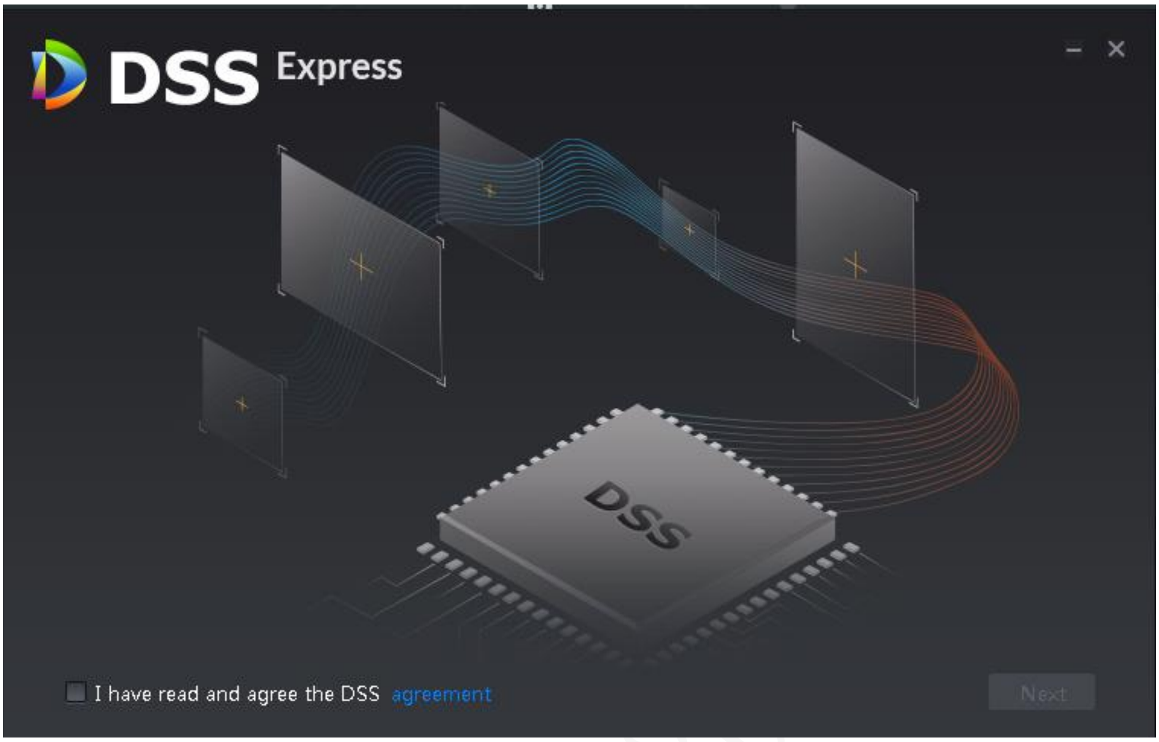
Step 2 Double-click ⊞, run or download client according to interface prompt.

Table 4-3 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 the client installation program under the save directory.

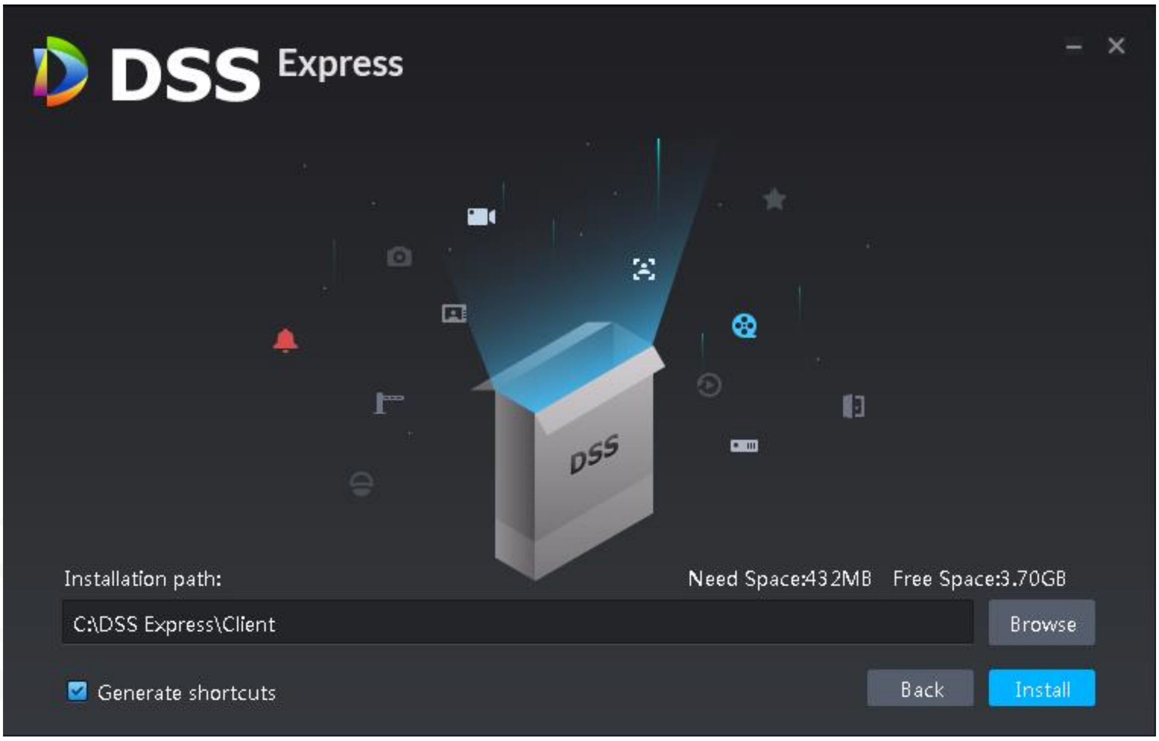
Figure 4-4 Confirm agreement



□ I have read and agree the DSS agreement

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

Figure 4-5 Select installation path



Installation path: Need Space:432MB Free Space:3.70GB

C:\DSS Express\Client

☑ Generate shortcuts

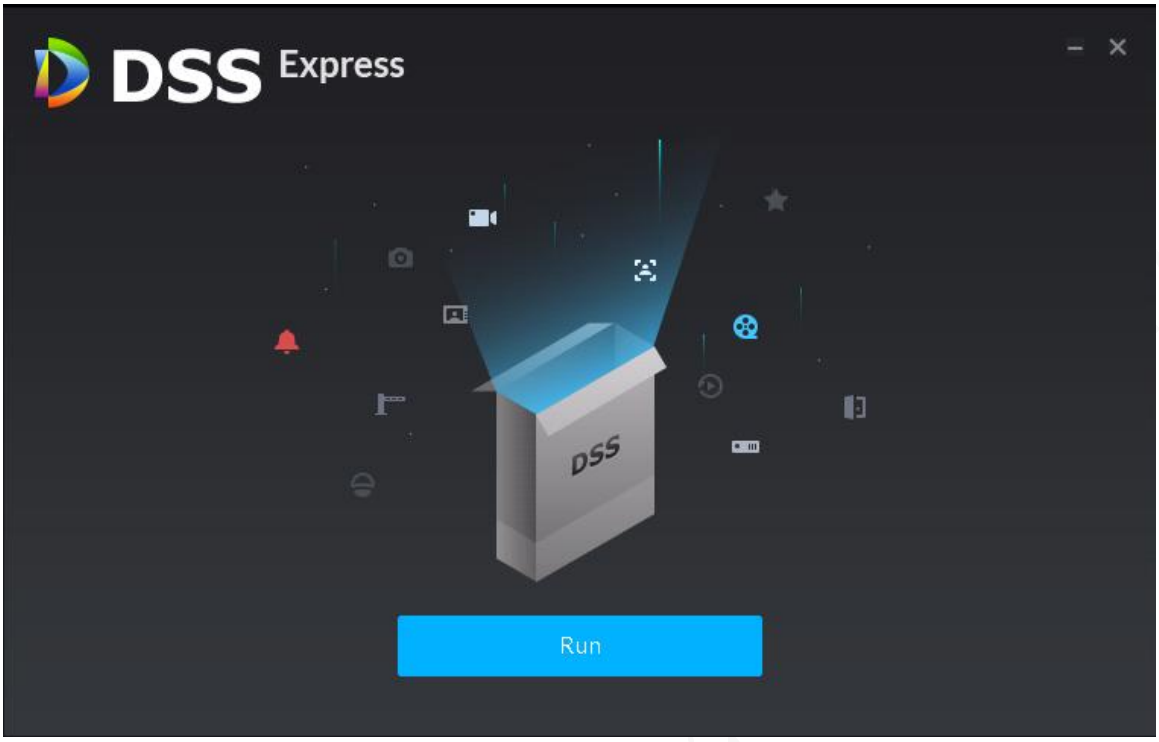
Step 5 Click **Browse** and select installation path, click **Install**.

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 4-6 Installation completed



## 4.1.3 Logging in to Express

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

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

Step 2 Click ︿, and then enter the server IP address.

Step 3 Enter username and password, and then click **Login**.

## 4.1.4 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**.

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.

# 4.2 Installing Face Recognition Terminal

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

The face recognition terminal can be applied to industrial park, scenic area, school, residential community and office building etc.

Face images can be imported to the device itself, besides, it supports using platform to issue faces to the terminal.

Figure 4-7 Scenario (1)

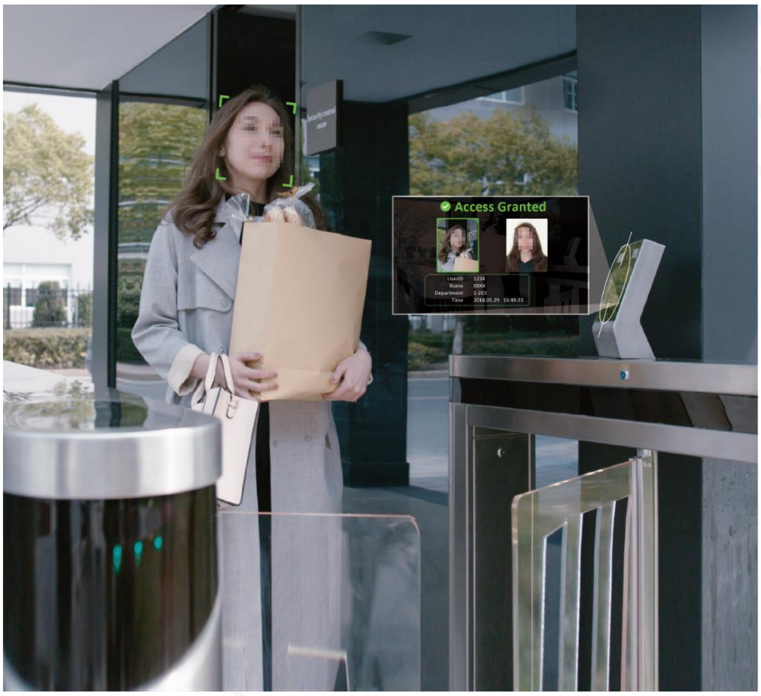


Figure 4-8 Scenario (2)

Figure 4-9 Scenario (3)

## 4.3 Installing DMSS

Use Google Play to download DMSS and then install it. For more info, see DMSS user's manual

# 5 Getting Started

Initialize your devices and then modify their IP addresses before you can use them.

## 5.1 Initializing NVR

You can initialize NVR either by following the on-screen instructions after you power it on for the first time, or by using ConfigTool.

Here we introduce how to initialize NVR with ConfigTool.

### 5.1.1 Initializing NVR with ConfigTool

Initialize your NVR with ConfigTool for first-time use. To acquire the 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 IP.

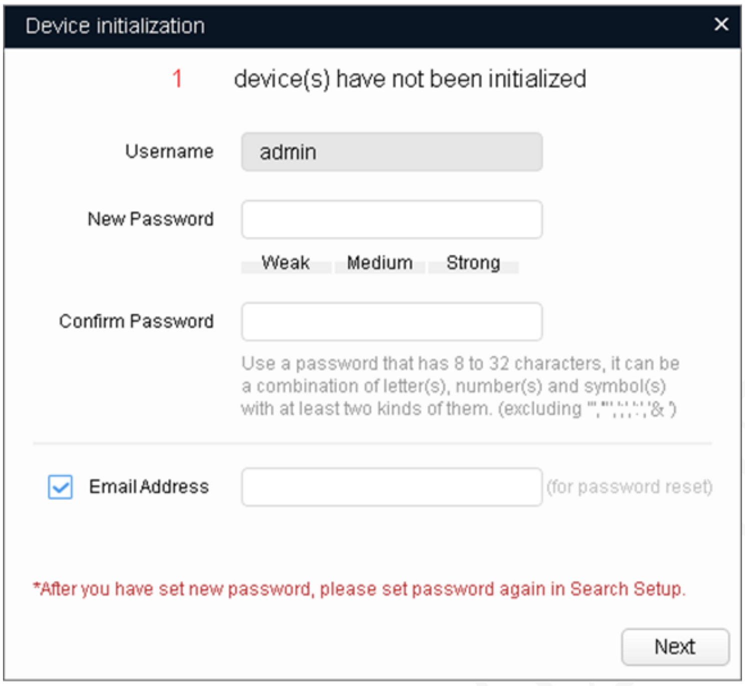
Step 3 Click **Search Setting**.

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 uninitialized NVRs, and then click **Initialize**.

Figure 5-1 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 6 Set and confirm the password, then enter a valid email address, and then click **Next**.

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

Step 7 Select the options according to your needs, and then click **OK**.

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

Step 8 Click **Finish**.

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

### 5.1.2 Modifying IP Address

- You can modify IP address of one or multiple NVRs 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.

You can initialize NVR either by following the on-screen instructions after you power it on for the first time, or by using ConfigTool.

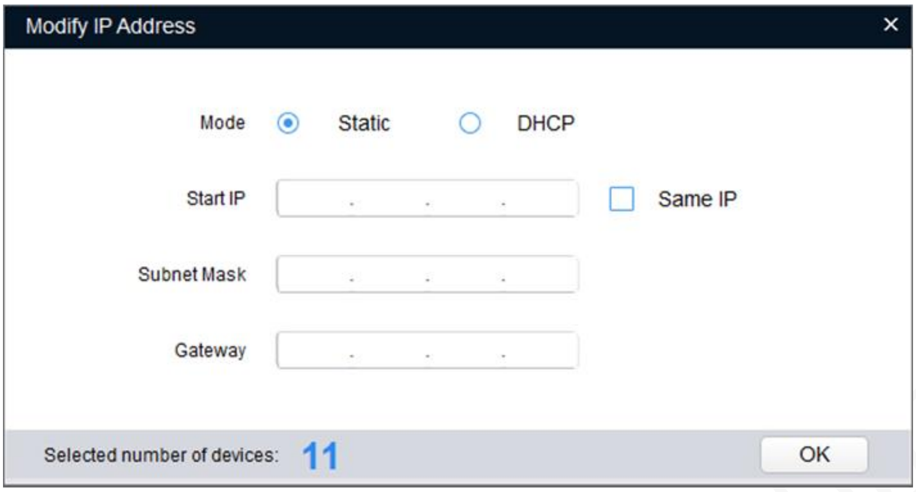
Here we introduce how to initialize NVR with ConfigTool.

Step 1 Do "Step 1" to "Step 5" in "5.1.1 Initializing NVR with ConfigTool " to search for NVRs 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 NVRs whose IP addresses need to be modified, and then click **Modify IP**.

Figure 5-2 Modify IP Address



Modify IP Address ×

Mode ● Static ○ DHCP

Start IP . . . □ Same IP

Subnet Mask . . .

Gateway . . .

Selected number of devices: 11

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**.

### 5.1.3 Updating System

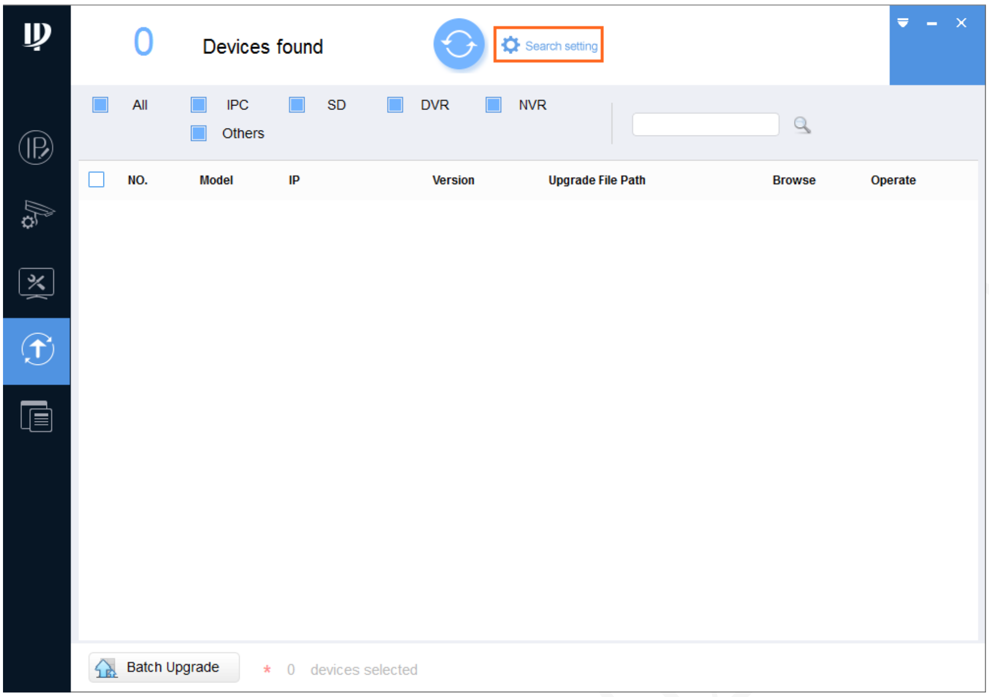
If the NVR version does not meet your requirement, you can update the NVR with ConfigTool. You can do that one by one or in batches.

- 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.

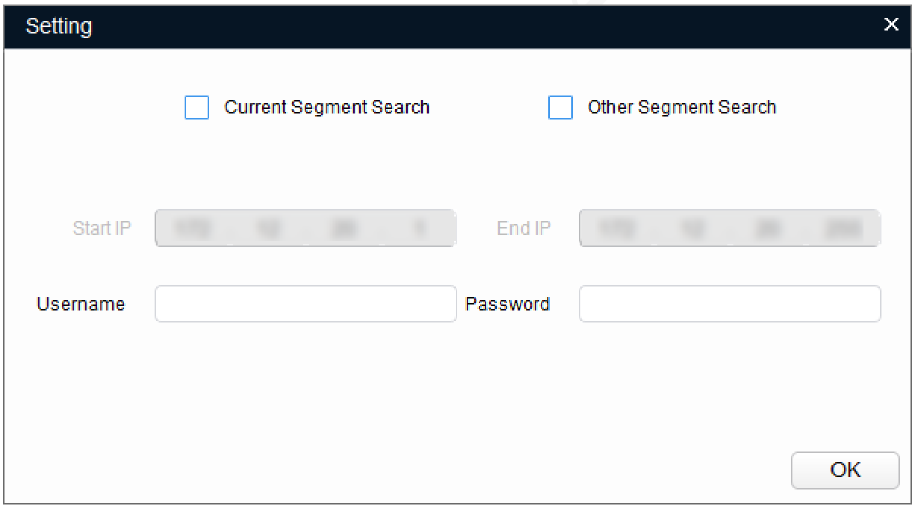
Step 2 Click ⬆.

Figure 5-3 Update



Step 3 Click **Search setting**.

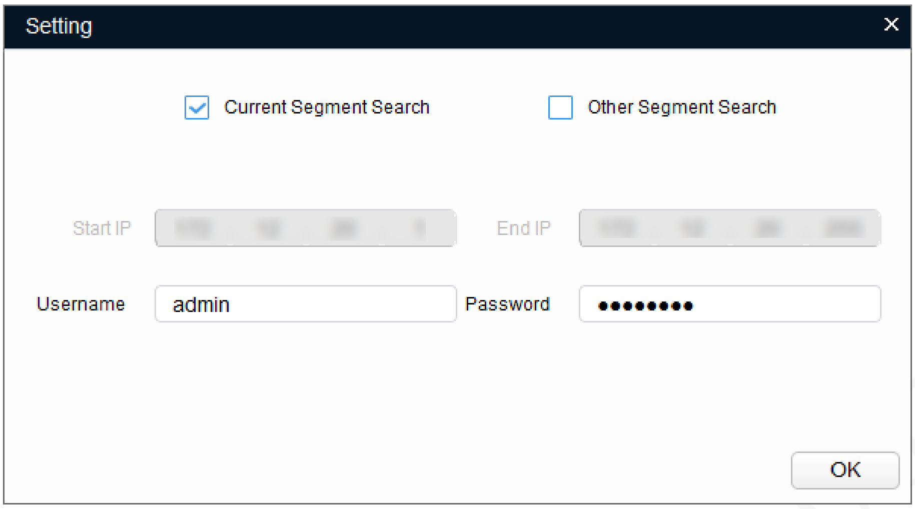
Figure 5-4 Search setting



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 5-5 Current segment search



Setting ×

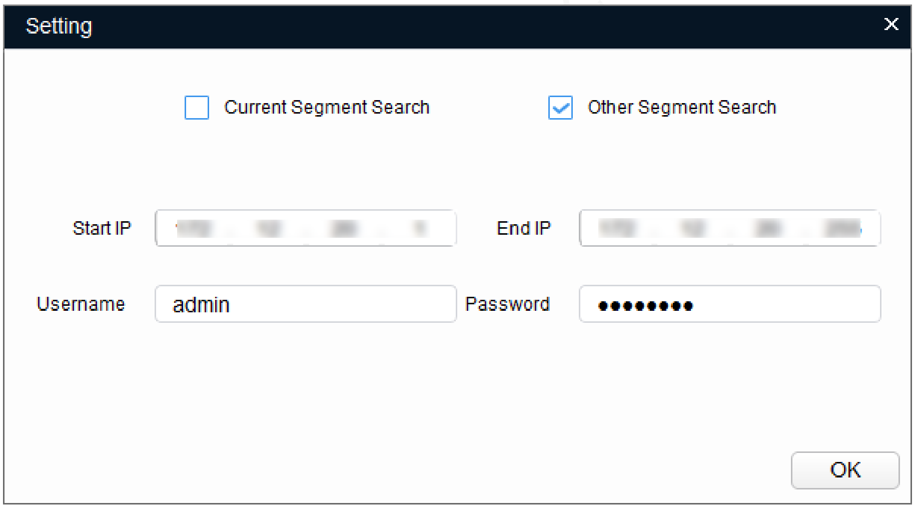
☑ Current Segment Search ☐ Other Segment Search

Start IP [redacted] End IP [redacted]

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 5-6 Other segment search



Setting ×

☐ Current Segment Search ☑ Other Segment Search

Start IP [redacted] End IP [redacted]

Username admin Password ••••••••

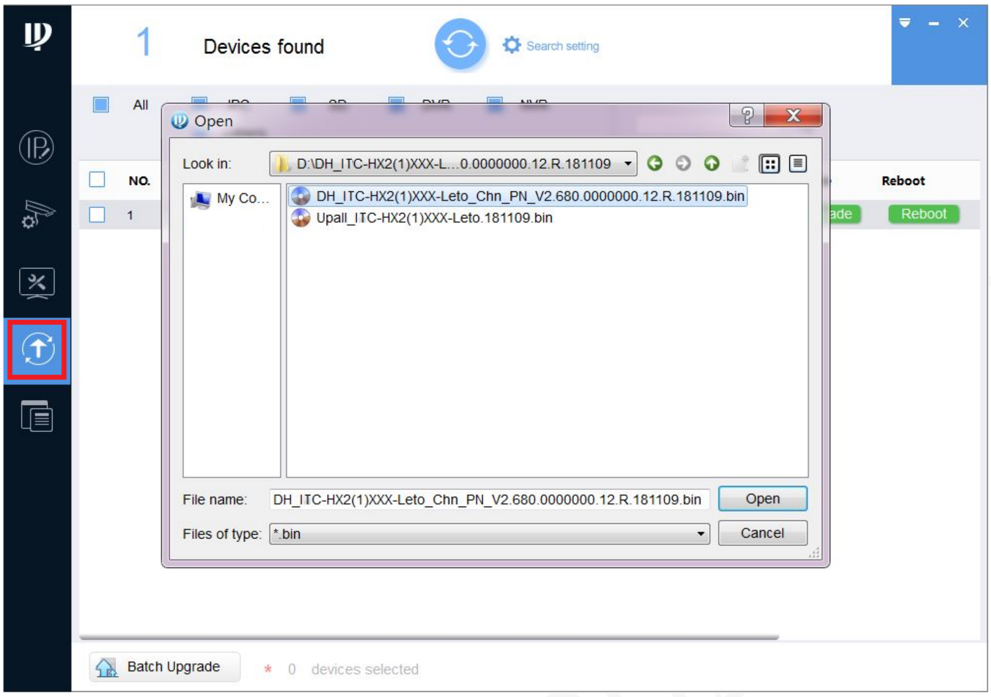
Step 5 Click **OK**.

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 5-7 Browse



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

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

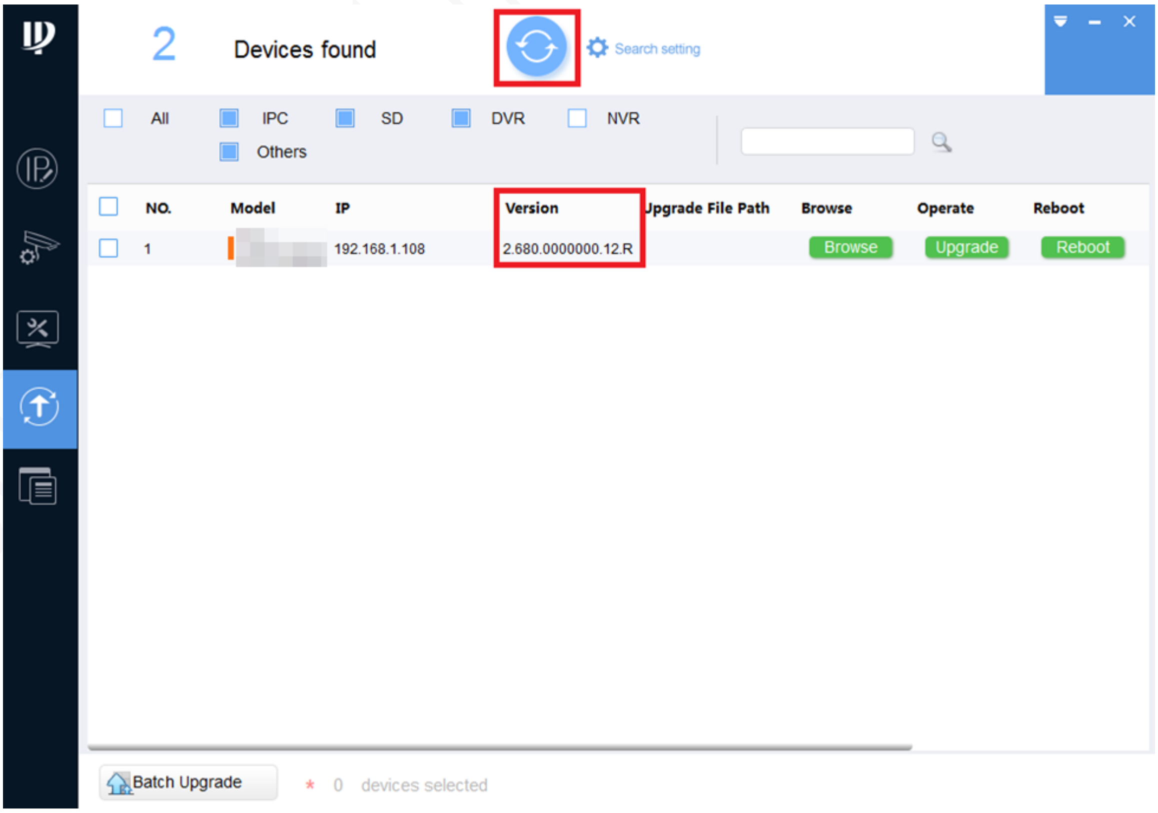
Files of type: *.bin

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 5-8 Confirm version



| NO. | Model | IP | Version | Upgrade 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 Face Recognition Terminal

You can initialize the face recognition terminal by following the on-screen instructions after you power it on for the first time, or use the ACS ConfigTool.

Here we introduce how to initialize the terminal with ACS ConfigTool.

### 5.2.1 Initializing Face Recognition Terminal with ACS ConfigTool

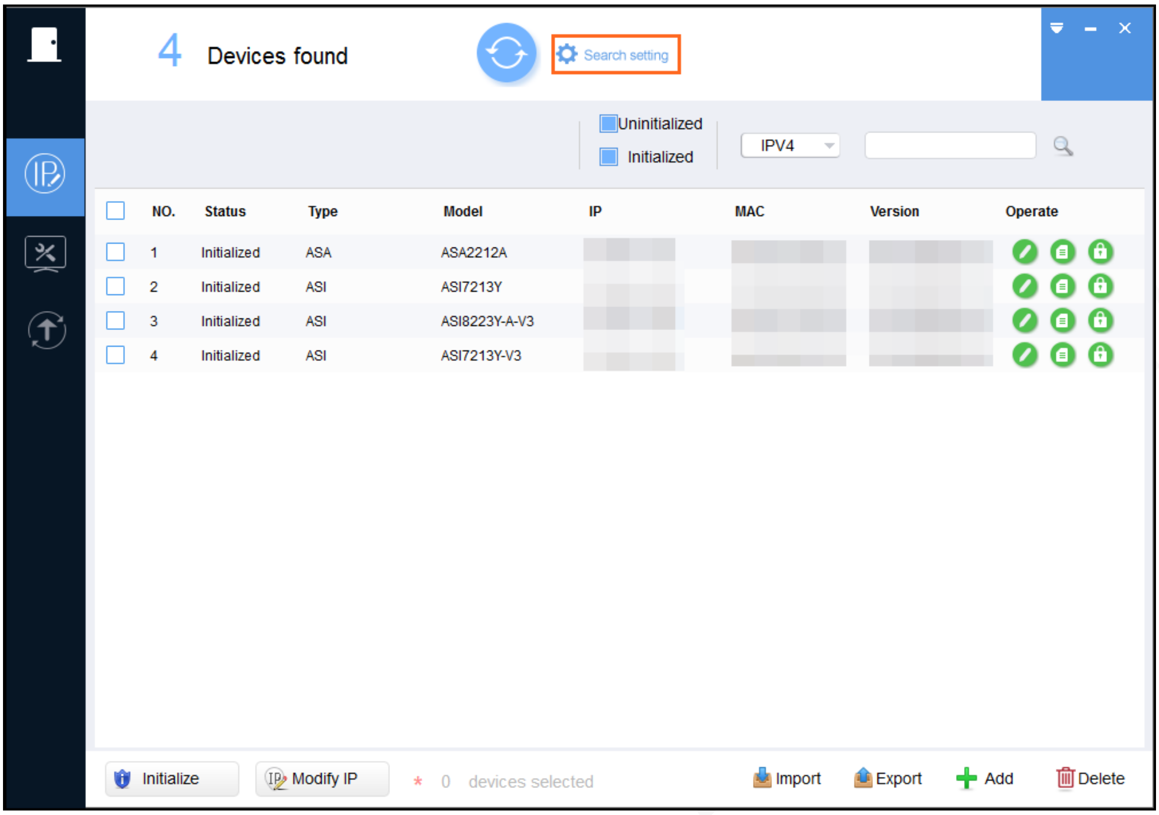
Initialize your face recognition terminal with ACS ConfigTool for first-time use. To acquire the tool, go to Dahua official website, and then select **Support > Download Center > ToolBox**, follow the on-screen instructions to download and install the tool.

- Device initialization is available on select models, and it is required at first use or after the device being reset.
- 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 "ACSConfig.exe" to open the tool.

Step 2 Click .

Figure 5-9 Modify IP



4 Devices found

Search setting

□ Uninitialized
□ Initialized

IPV4

| □ | NO. | Status | Type | Model | IP | MAC | Version | Operate |
|---|---|---|---|---|---|---|---|---|
| □ | 1 | Initialized | ASA | ASA2212A | [redacted] | [redacted] | [redacted] | |
| □ | 2 | Initialized | ASI | ASI7213Y | [redacted] | [redacted] | [redacted] | |
| □ | 3 | Initialized | ASI | ASI8223Y-A-V3 | [redacted] | [redacted] | [redacted] | |
| □ | 4 | Initialized | ASI | ASI7213Y-V3 | [redacted] | [redacted] | [redacted] | |

Initialize   Modify IP   * 0 devices selected   Import   Export   Add   Delete

Step 3 Click **Search setting**.

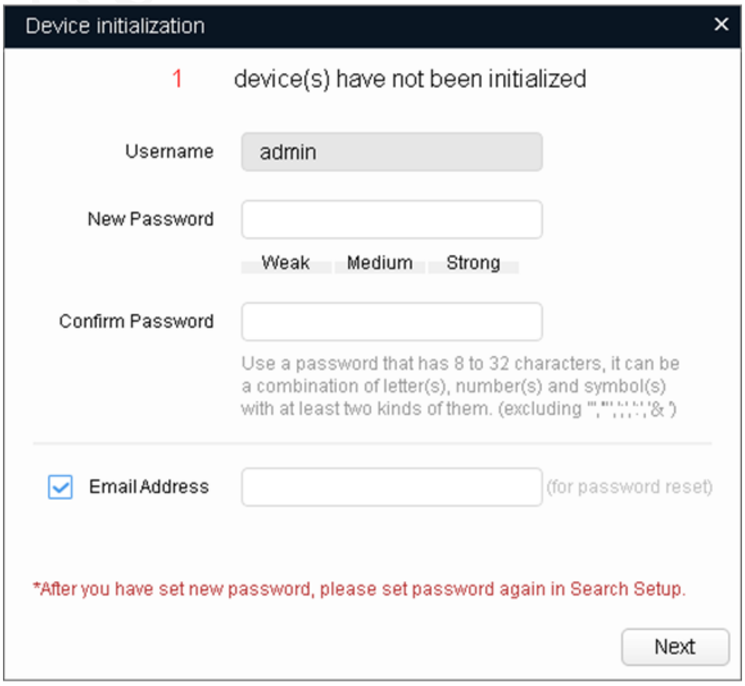
Step 4 Enter the start IP address and end IP address of the network segment in which you want to search devices, and then click **OK**.

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 5-10 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.

Next

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**.

The **Initialization** interface is displayed after initialization is completed. 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**.

## 5.2.2 Modifying IP Address

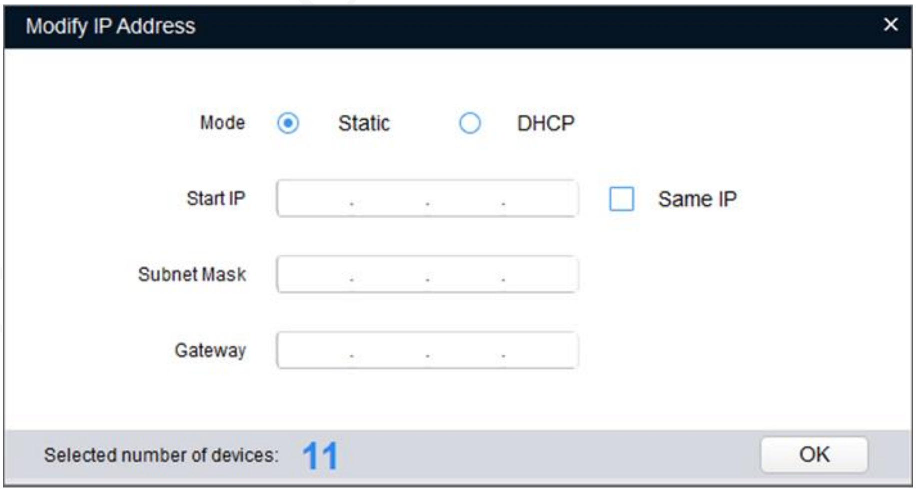
- You can modify IP address of one or multiple devices in one time. This section is based on modifying IP addresses in batches.
- Modifying IP addresses in batches is available only when the corresponding devices have the same login username and password.

Step 1 Do "Step 1" to "Step 4" in "5.2.1 Initializing Face Recognition Terminal with ACS ConfigTool" to search for the face recognition terminals 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 whose IP addresses need to be modified, and then click **Modify IP**.

Figure 5-11 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**.

### 5.2.3 Updating System

ACSConfig supports updating devices one by one or in batches.

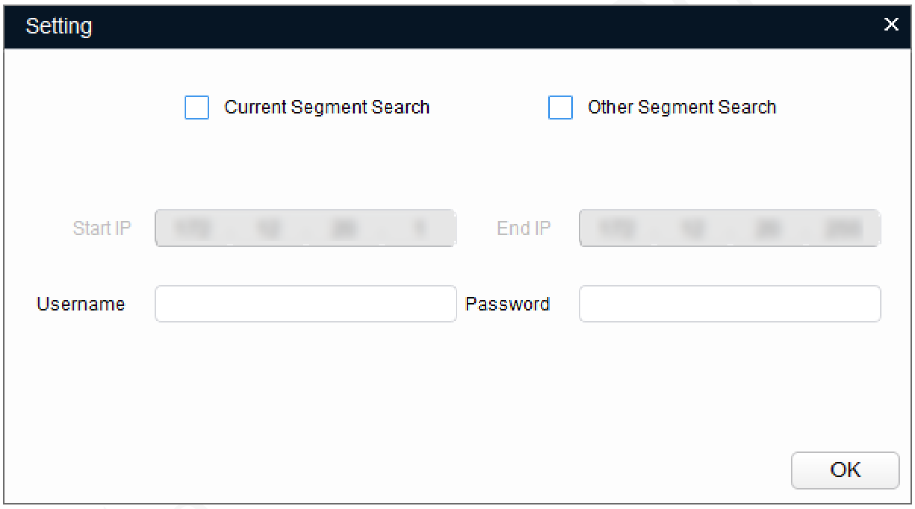
- Updating devices one by one is ideal when few devices are involved, and login username and password of the devices are different.
- Updating devices in batches is recommended when multiple devices are involved, and login username and passwords of cameras are the same.

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

Step 2 Click ⬆.

Step 3 Click **Search setting**.

Figure 5-12 Search setting



Setting

☐ Current Segment Search ☐ Other Segment Search

Start IP End IP

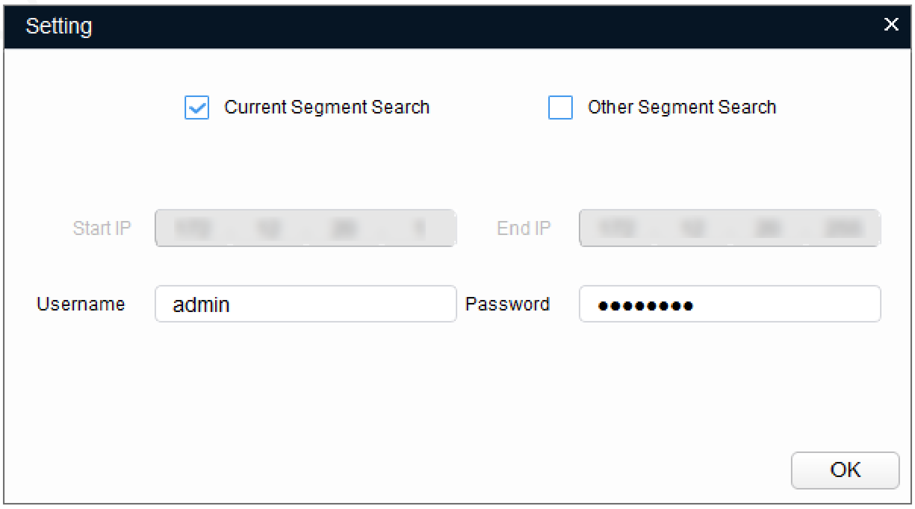
Username Password

OK

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 5-13 Current segment search



Setting

☑ Current Segment Search ☐ Other Segment Search

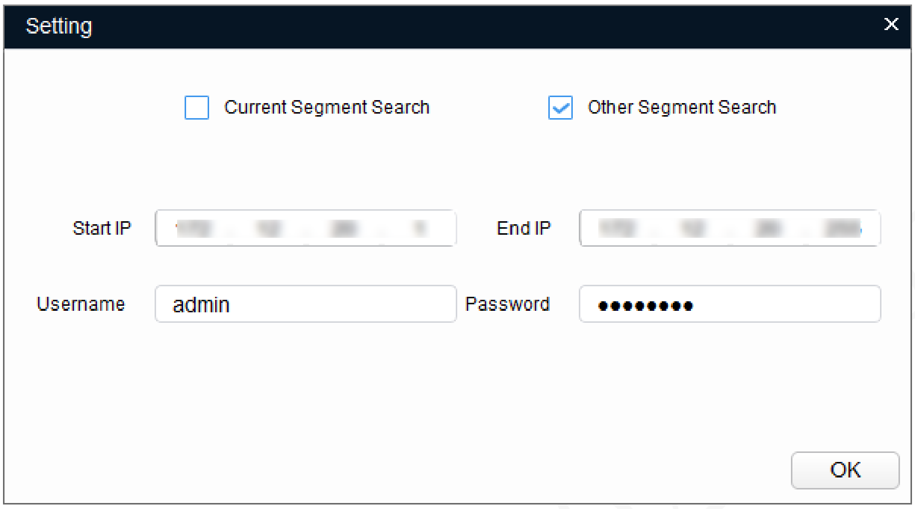
Start IP End IP

Username admin Password ••••••••

OK

- 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 5-14 Other segment search



Setting ✕

□ Current Segment Search ☑ Other Segment Search

Start IP [redacted] End IP [redacted]

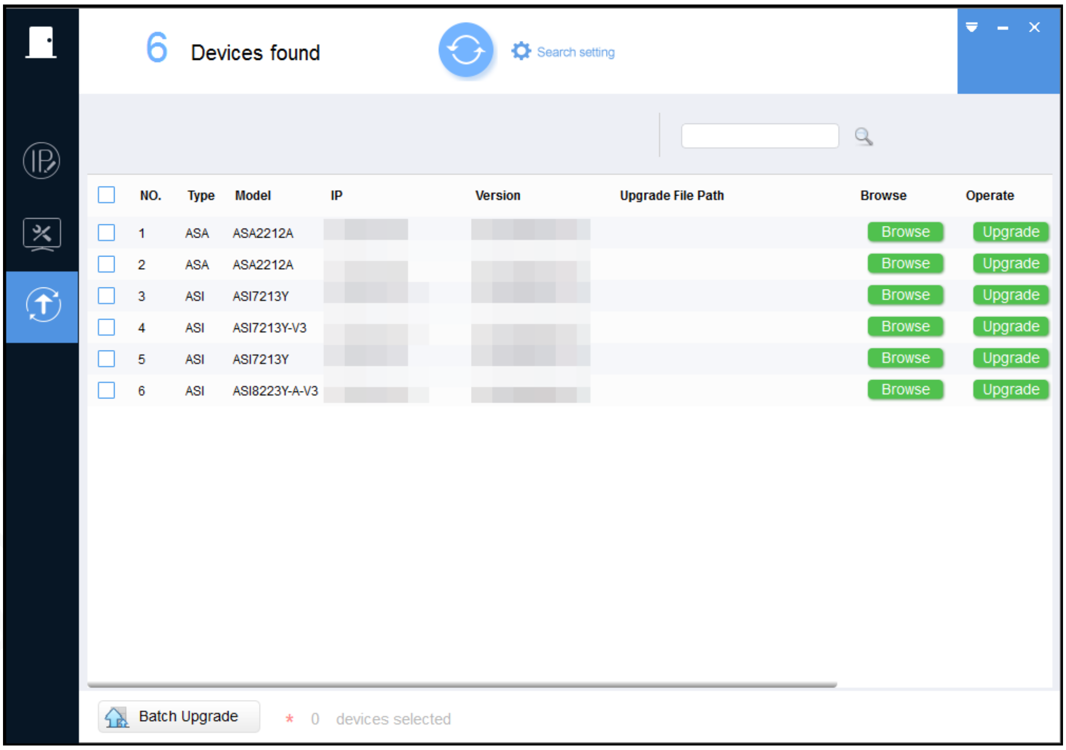
Username admin Password ●●●●●●●●●

OK

Step 5 Click **OK**.

The search result is displayed.

Figure 5-15 Search result



6 Devices found

Search setting

| □ | NO. | Type | Model | IP | Version | Upgrade File Path | Browse | Operate |
|---|---|---|---|---|---|---|---|---|
| □ | 1 | ASA | ASA2212A | [redacted] | [redacted] | | Browse | Upgrade |
| □ | 2 | ASA | ASA2212A | [redacted] | [redacted] | | Browse | Upgrade |
| □ | 3 | ASI | ASI7213Y | [redacted] | [redacted] | | Browse | Upgrade |
| □ | 4 | ASI | ASI7213Y-V3 | [redacted] | [redacted] | | Browse | Upgrade |
| □ | 5 | ASI | ASI7213Y | [redacted] | [redacted] | | Browse | Upgrade |
| □ | 6 | ASI | ASI8223Y-A-V3 | [redacted] | [redacted] | | Browse | Upgrade |

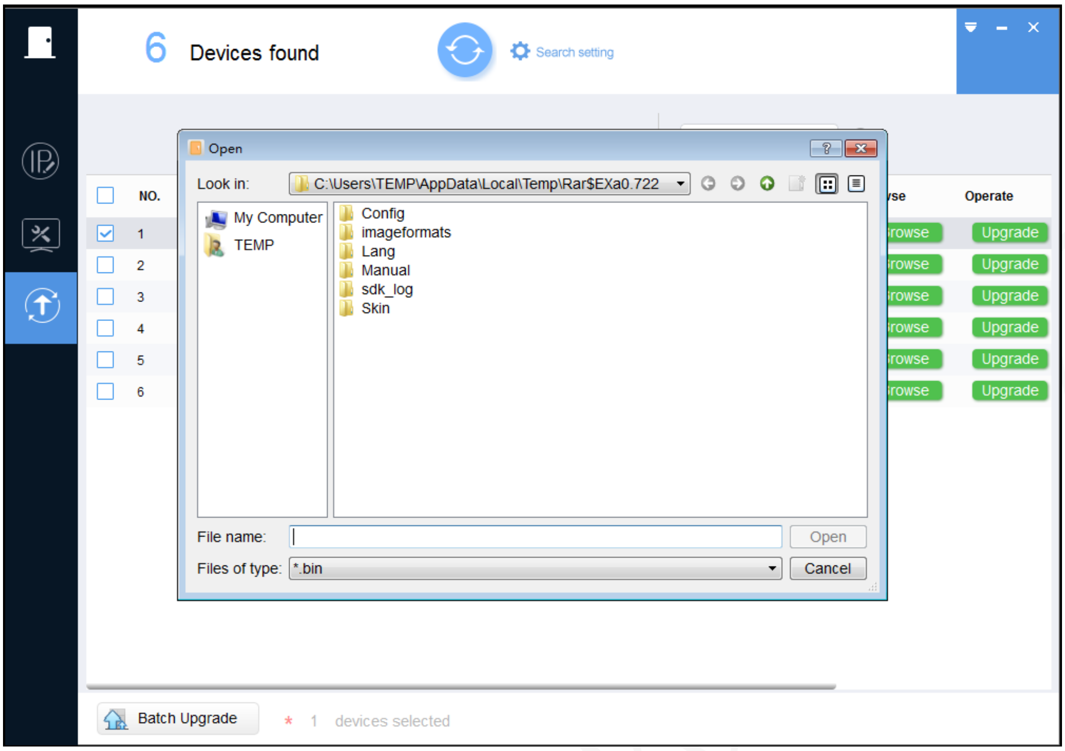
Batch Upgrade * 0 devices selected

Step 6 Select the device to update.

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

Step 7 Select the update file.

Figure 5-16 Select update file



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. 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.

# 6 Configuration and Commissioning

Configure the basic settings, and then carry out commissioning to make sure that your configurations are correct.

Skip irrelevant sections if you do not use the corresponding product. For example, if you do not use NVR, skip "6.2 Configuring NVR."

## 6.1 Configuring Face Recognition Terminal

To achieve access control by face recognition, temperature monitoring and mask detection, you need to set and enable the relevant parameters, and create face database on the terminal.

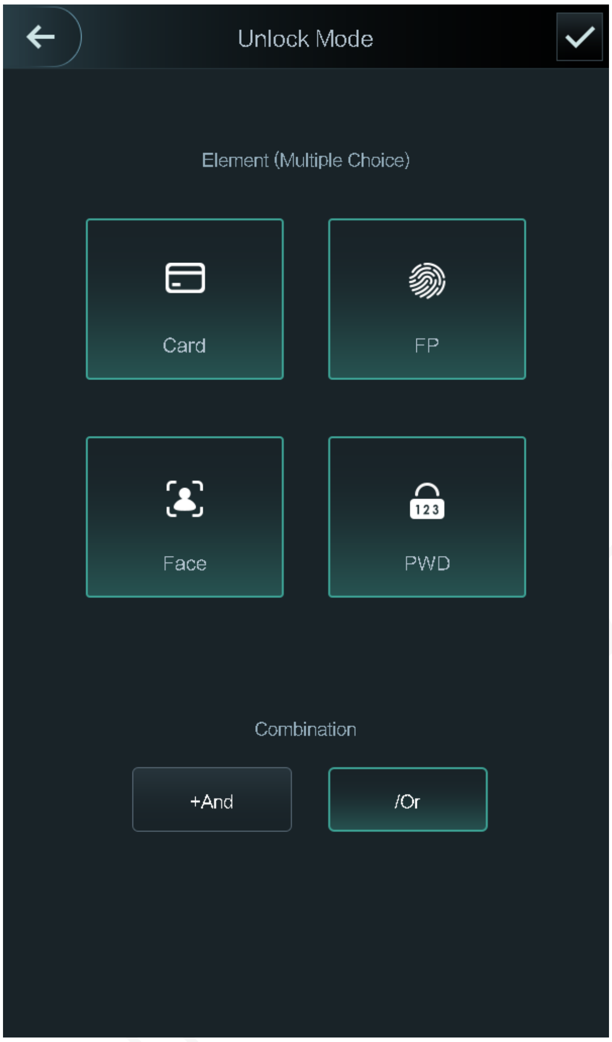
### 6.1.1 Configuring Unlock Mode

Enable opening door by face recognition. If you use Express in your solution, enable both the face recognition and card modes.

Step 1 On the local interface of the face recognition terminal, tap ⊞ **>** admin to log in.

Step 2 Select **Access > Unlock Mode > Unlock Mode**.

Figure 6-1 Unlock modes



Step 3 Tap the mode you need. For example, **Face**, or **Face** and **Card**.

Step 4 Tap ✓ to save the settings.

## 6.1.2 Creating Face Database

Create a face database (by USB flash or by Express) to the face recognition terminal to let the terminal compare the detected faces against the face database for access control accordingly.

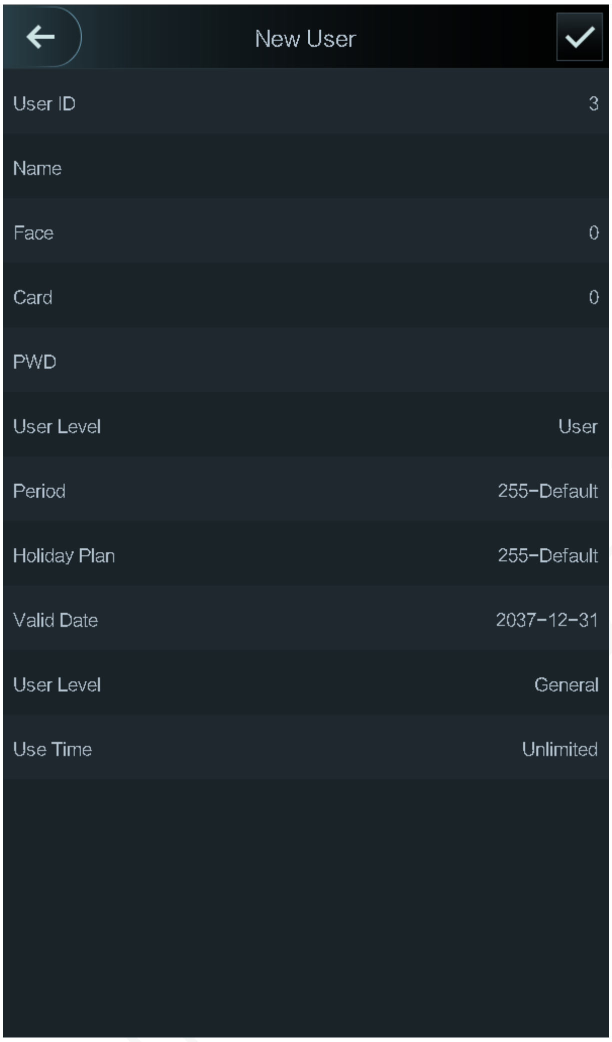
If you use Express in your solution, skip this section and refer to "6.3.5 Configuring People Information."

Step 1 Register face images on one face recognition terminal to create the first face database.

1) On the local interface of the face recognition terminal, tap ⊞ > admin to log in.

2) Tap **User > New User**, and then set user ID, name and level.

Figure 6-2 New User Info



| | |
|---|---|
| User ID | 3 |
| Name | |
| Face | 0 |
| Card | 0 |
| PWD | |
| User Level | User |
| Period | 255-Default |
| Holiday Plan | 255-Default |
| Valid Date | 2037-12-31 |
| User Level | General |
| Use Time | Unlimited |

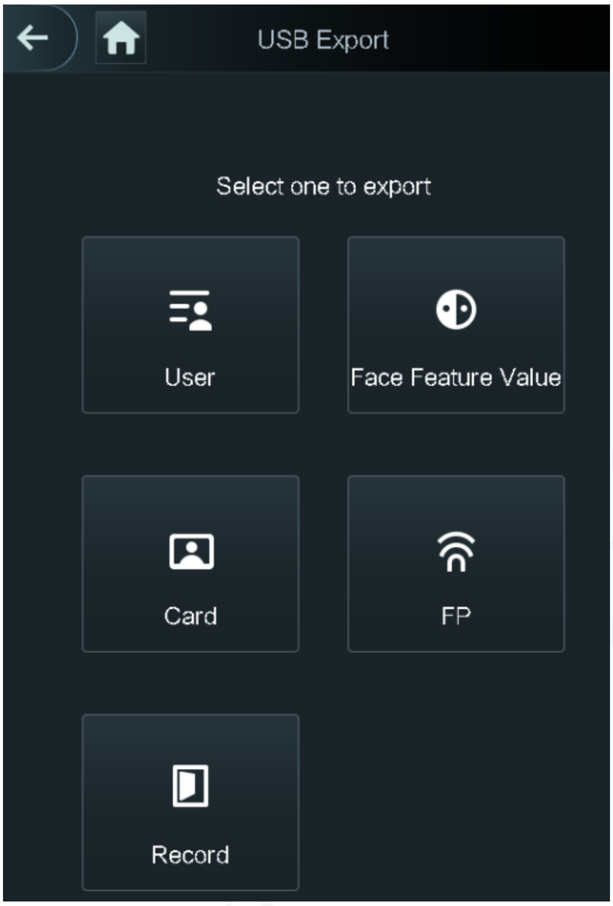
3) Tap **Face**, and then take a face picture.
Make sure that your face is centered on the face frame and the access controller will automatically take a face picture.

4) Perform 1) to 3) to collect face images of all the users you need to add. For example, collect face images of all the students.

Step 2 Export the face database, and then import it to other face recognition terminals.

1) Prepare a USB disk.
2) Insert it to the face recognition terminal which has the first face database, and then log in to the face recognition terminal locally.
3) Select USB > USB Export.

Figure 6-3 USB Import



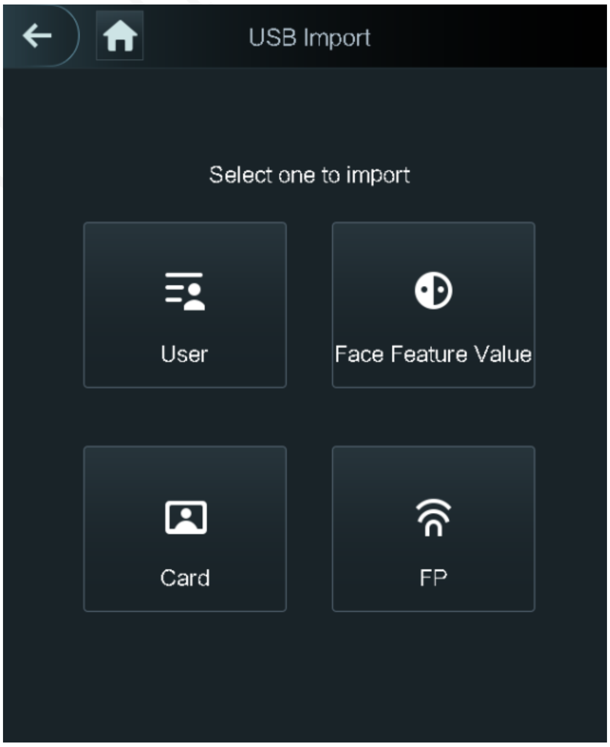
USB Export

Select one to export

4) Tap **Face Feature Value**, and then tap **OK**.

Face images in the terminal will be exported into the USB disk.

Figure 6-4 USB Import



USB Import

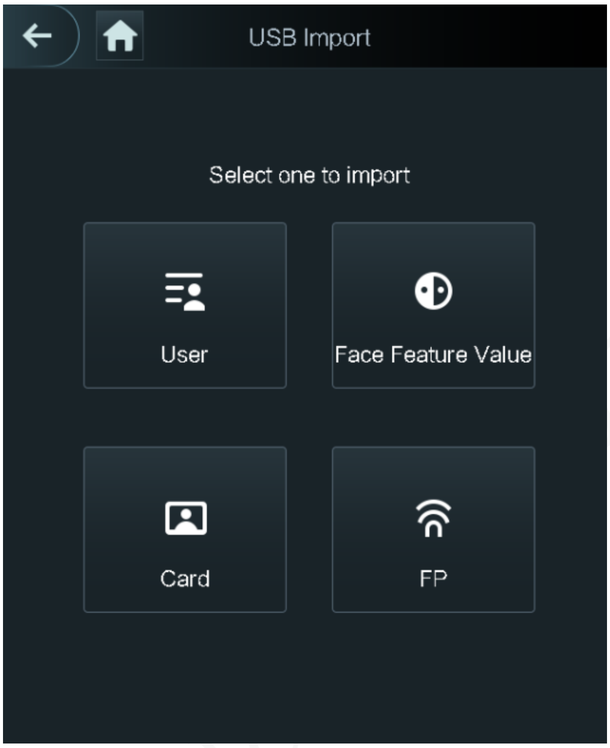
Select one to import

Step 3 Import the face database to other face recognition terminals one by one.

Insert the USB disk that has the first face database into another face recognition terminal, and then perform the following steps to import the database.

1) On the local interface, tap ⊞ **>** admin to log in.
2) Tap USB > USB Import.

Figure 6-5 USB Import



3) Tap **Face Feature Value**, and then tap **OK**.
   Face images in the USB disk will be imported into the terminal.

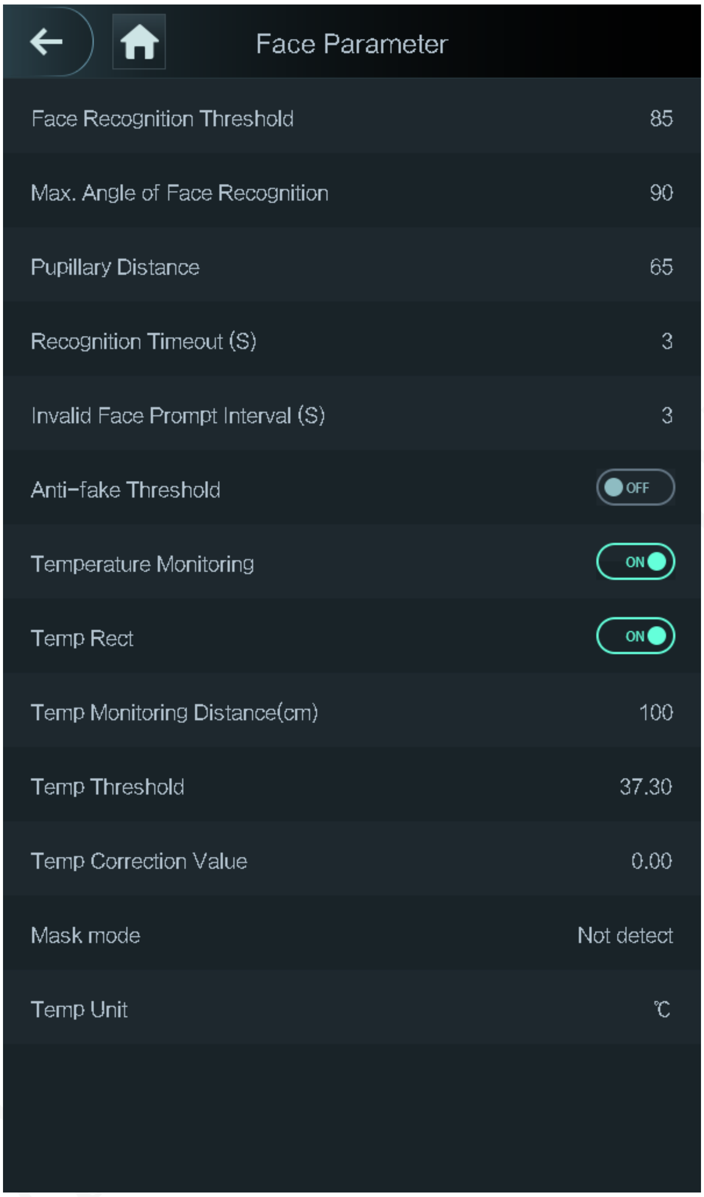
### 6.1.3 Configuring Face Recognition Parameters

Set basic face recognition parameters, and enable temperature monitoring and mask detection.

Step 1 On the local interface of the face recognition terminal, tap ⊞ **>** admin to log in.

Step 2 Tap **System > Face Parameter**.

Figure 6-6 Face parameter (local interface)



Face Parameter

| | |
|---|---|
| Face Recognition Threshold | 85 |
| Max. Angle of Face Recognition | 90 |
| Pupillary Distance | 65 |
| Recognition Timeout (S) | 3 |
| Invalid Face Prompt Interval (S) | 3 |
| Anti-fake Threshold | OFF |
| Temperature Monitoring | ON |
| Temp Rect | ON |
| Temp Monitoring Distance(cm) | 100 |
| Temp Threshold | 37.30 |
| Temp Correction Value | 0.00 |
| Mask mode | Not detect |
| Temp Unit | ℃ |

Step 3 Set the following parameters. For the introduction to more parameters on the **Face Parameter** interface, see the user's manual.

Table 6-1 Face detect parameter description

| Parameter | Description |
|---|---|
| Anti-fake Threshold | Keep it off (OFF) here.<br>This function prevents people from unlocking by human face images or human face models. |

| | |
|---|---|
| Temperature Monitoring | Tap the OFF that corresponds to **Temperature Monitoring** , and then set the following parameters.<br>● Temp Unit: Select a temperature unit between °C and °F.<br>● Temp Rect: Set whether to display the temperature monitoring box or not.<br>● Temp Monitoring Distance (cm): The value is 0 by default. Set other values to enable temperature monitoring within a defined distance. 80 cm is recommended.<br>● Temp Threshold (°C): Set the temperature threshold. The monitored body temperature will be judged as high temperature if it is greater than or equal to the set value.<br>● Temp Correction Value: This parameter is for testing. The difference of the temperature monitoring environment might cause the temperature deviation between the monitored temperature and the actual temperature. You can select multiple monitored samples for testing. According to the comparison between the monitored temperature and the actual temperature, you can correct the temperature deviation by this parameter. For example, if the monitored temperature is 0.5°C lower than the actual temperature, the correction value is set to 0.5°C; if the measured temperature is 0.5°C higher than the actual temperature, the correction value is set to -0.5°C.<br>📖<br>Only the terminal with a temperature monitoring unit supports this parameter. |
| Mask Mode | Tap **Mask Mode**, and then select **Mask reminder** or **Mask intercept**.<br>● Mask reminder: Mask is detected during face recognition. If the person is detected not wearing a mask, the system will prompt mask reminder and passage is allowed.<br>● Mask intercept: Mask is detected during face recognition. If the person is detected not wearing a mask, the system will prompt mask reminder and passage is not allowed. |

Step 4 Tap ✓.

## 6.1.4 Commissioning

### 6.1.4.1 Face Recognition, Temperature Measurement and Mask Detection

Preparation

- Face recognition terminal is correctly installed and connected.
- Face recognition terminal is correctly initialized.
- Face database, face recognition parameters are correctly configured.

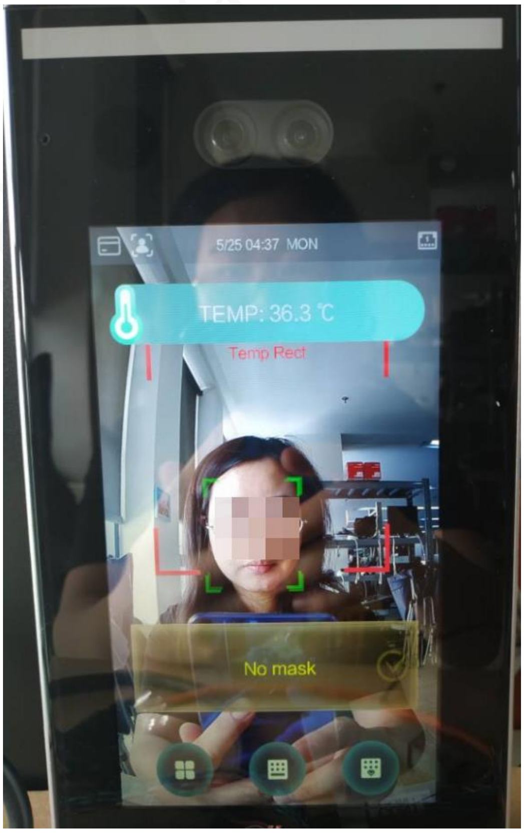
Objectives

The face recognition terminal can correctly recognize human face, measure face temperature, and detect mouth mask.

Procedure

Stand in front of the face recognition terminal, and check whether the screen shows face recognition result and temperature value, and whether it warns of mask absence.

Figure 6-7 Face verification



### 6.1.4.2 Normal Body Temperature

Preparation

- Face recognition terminal and turnstile are correctly installed and connected.
- Face recognition terminal is correctly initialized.
- Unlock mode, face database, face recognition parameters are correctly configured.

Objectives

The turnstile opens when a person with normal body temperature is recognized.

Procedure

For a person with normal temperature (within the temperature threshold, check how to set threshold value in "6.1.3 Configuring Face Recognition Parameters"), check whether the face recognition terminal opens the turnstile. Make sure the face image of the person is in the database. If not, register face image first.

### 6.1.4.3 Elevated Body Temperature

Preparation

- Face recognition terminal and turnstile are correctly installed and connected.
- Face recognition terminal is correctly initialized.
- Unlock mode, face database, face recognition parameters are correctly configured.

Objectives

The turnstile keeps closed and the face recognition shows an alarm when a person with a fever is recognized.

Procedure

For a person with a fever (body temperature higher than the temperature threshold, check how to set threshold value in "6.1.3 Configuring Face Recognition Parameters"), check whether the face recognition terminal displays the alarm correctly and keeps the turnstile closed. Make sure the face image of the person is in the database. If not, register face image first.

### 6.1.4.4 Mask Detection

#### Preparation

- Face recognition terminal and turnstile are correctly installed and connected.
- Face recognition terminal is correctly initialized.
- Unlock mode, face database, face recognition parameters are correctly configured.

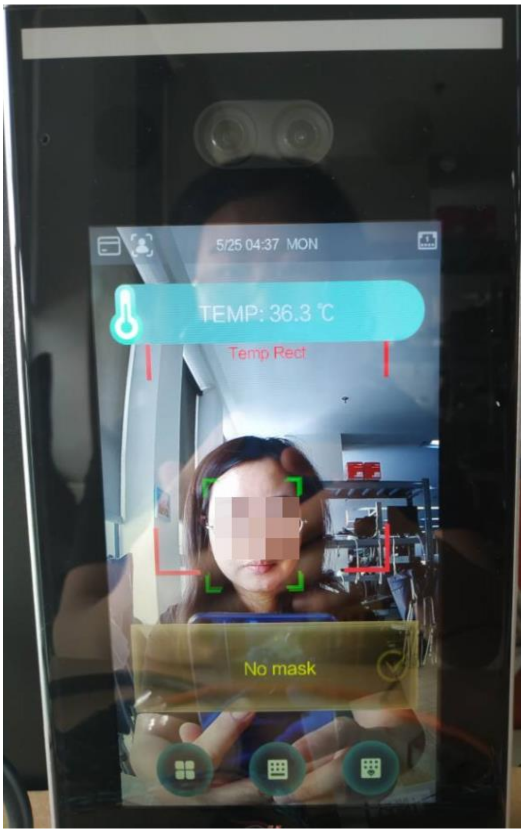
#### Objectives

The turnstile keeps closed, or the face recognition terminal gives a warning when a person is detected wearing no mouth mask.

#### Procedure

- If you have selected **Mask intercept** for **Mask mode** (see "6.1.3 Configuring Face Recognition Parameters"), the turnstile should keep closed when a person is detected wearing no mouth mask.
- If you have selected **Mask reminder** for **Mask mode**, the turnstile should give a warning of mask absence when the face recognition terminal detects a person wearing no mask.

Figure 6-8 Mouth mask detection



# 6.2 Configuring NVR

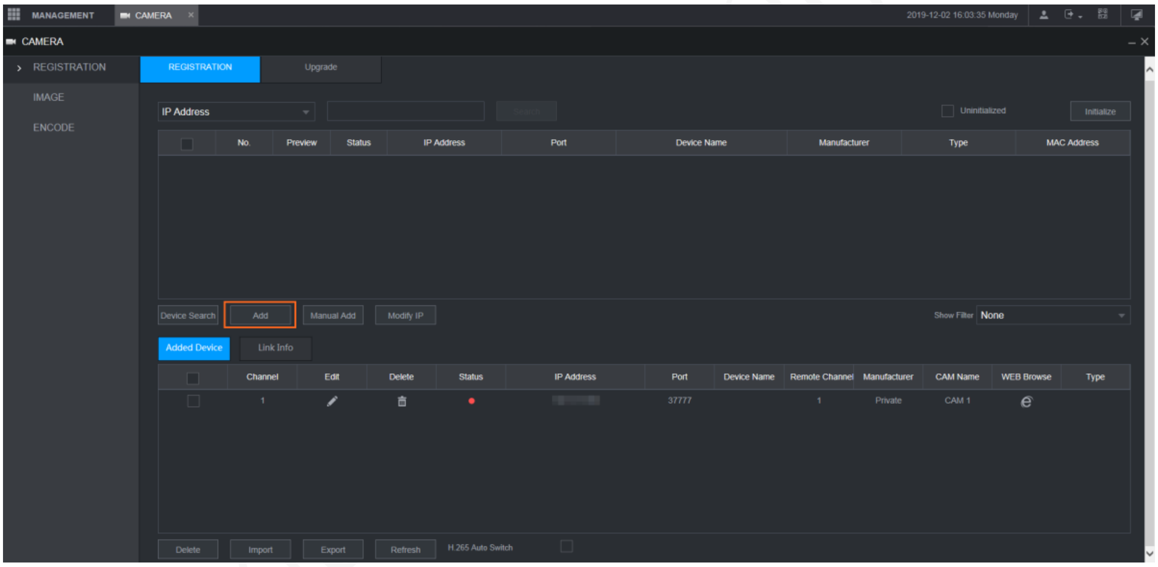
To monitor face recognition, temperature measurement and mouth mask, you need to add the face recognition terminal to NVR, and enable those functions.

You cannot create face database on NVR. For the "face recognition terminal – NVR" solution, you need to create face database on the face recognition terminal. For details, see "6.1.2 Creating Face Database."

## 6.2.1 Adding Face Recognition Terminal to NVR

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

Figure 6-9 Add face recognition terminal (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 | | |

Step 2 Add a device.

You can add the face recognition terminal through Auto Scan and Manual Add.

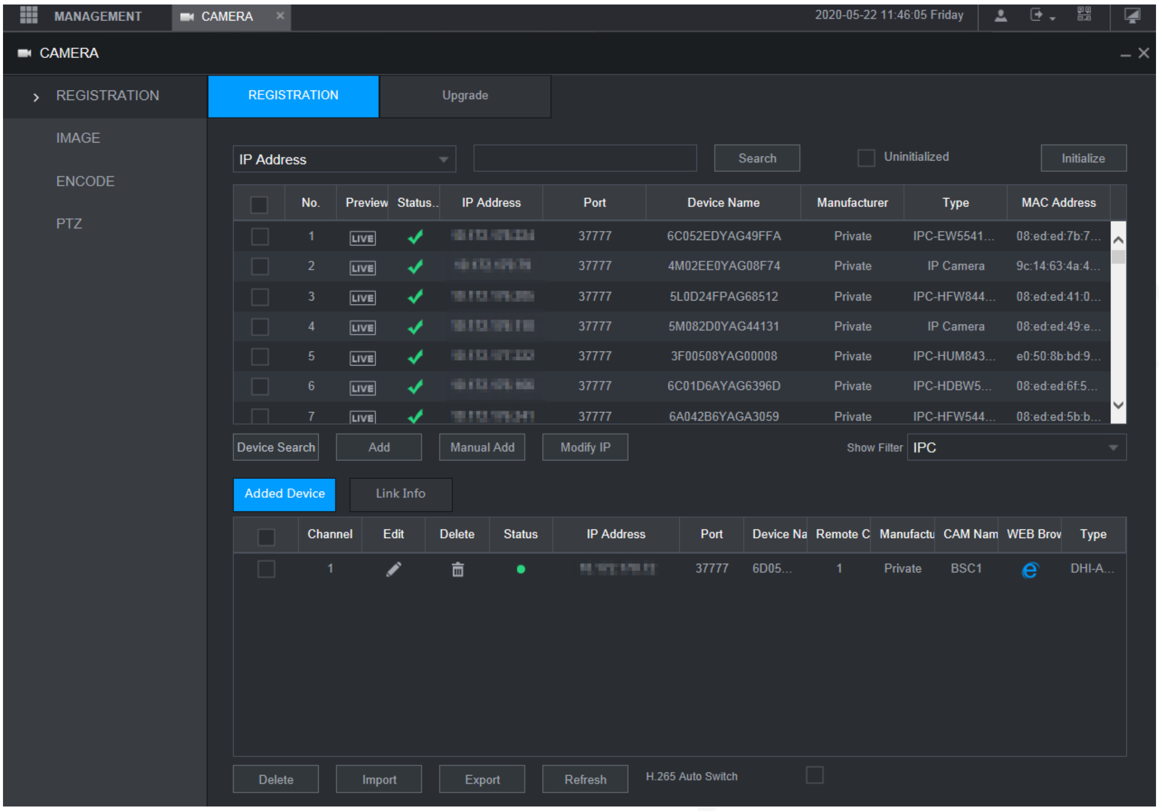
- Auto Scan

  Click Device Search.

  The devices that can be searched will be displayed.

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

Figure 6-10 Add face recognition terminal (2)



| □ | No. | Preview | Status.. | IP Address | Port | Device Name | Manufacturer | Type | MAC Address |
|---|---|---|---|---|---|---|---|---|---|
| □ | 1 | LIVE | ✓ | [redacted] | 37777 | 6C052EDYAG49FFA | Private | IPC-EW5541... | 08:ed:ed:7b:7... |
| □ | 2 | LIVE | ✓ | [redacted] | 37777 | 4M02EE0YAG08F74 | Private | IP Camera | 9c:14:63:4a:4... |
| □ | 3 | LIVE | ✓ | [redacted] | 37777 | 5L0D24FPAG68512 | Private | IPC-HFW844... | 08:ed:ed:41:0... |
| □ | 4 | LIVE | ✓ | [redacted] | 37777 | 5M082D0YAG44131 | Private | IP Camera | 08:ed:ed:49:e... |
| □ | 5 | LIVE | ✓ | [redacted] | 37777 | 3F00508YAG00008 | Private | IPC-HUM843... | e0:50:8b:bd:9... |
| □ | 6 | LIVE | ✓ | [redacted] | 37777 | 6C01D6AYAG6396D | Private | IPC-HDBW5... | 08:ed:ed:6f:5... |
| □ | 7 | LIVE | ✓ | [redacted] | 37777 | 6A042B6YAGA3059 | Private | IPC-HFW544... | 08:ed:ed:5b:b... |

| □ | Channel | Edit | Delete | Status | IP Address | Port | Device Na | Remote C | Manufactu | CAM Nam | WEB Brov | Type |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | 1 | ✎ | 🗑 | ● | [redacted] | 37777 | 6D05... | 1 | Private | BSC1 | e | DHI-A... |

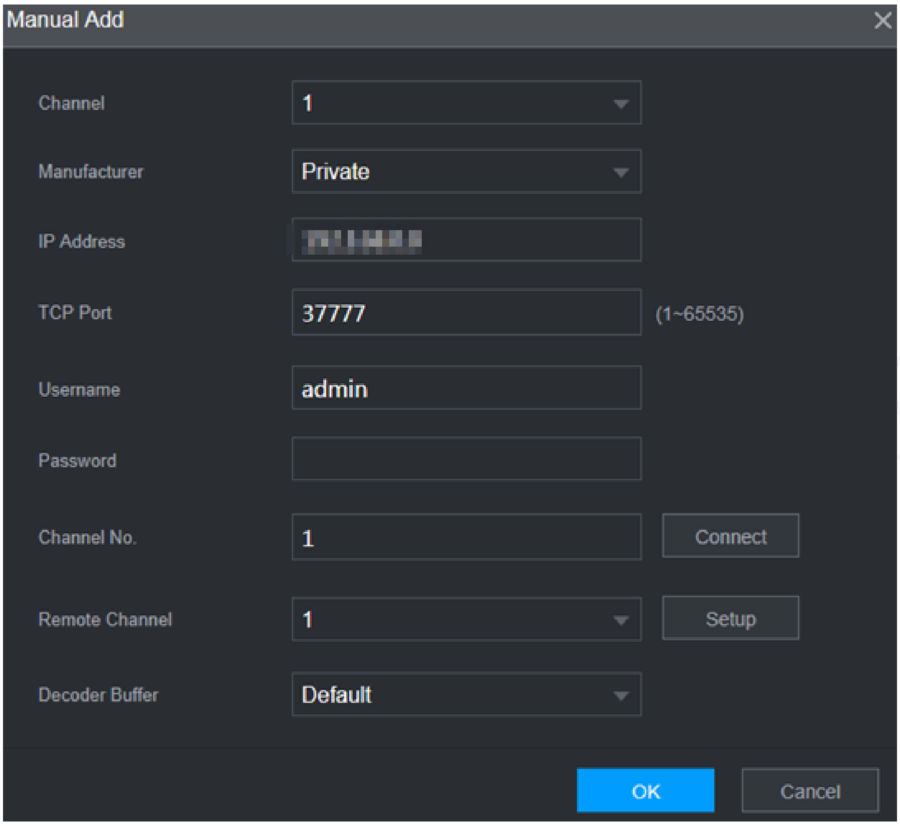
Table 6-2 Parameter description

| 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

1) Click Manual Add.

Figure 6-11 Manual add



Manual Add

Channel: 1

Manufacturer: Private

IP Address: [redacted]

TCP Port: 37777 (1~65535)

Username: admin

Password:

Channel No.: 1

Remote Channel: 1

Decoder Buffer: Default

2) Set parameters.

Table 6-3 Manual add parameters

| Parameter | Description |
|---|---|
| Channel | Displays the channel No. on your NVR to which you connect the target device to. |
| Manufacturer | Select **Private**.<br>📖<br>Supported protocol might vary with different models, and the actual product shall prevail. |
| IP Address | Enter the IP address of the device. |
| TCP Port | Transmission control protocol port, the value is 37777 by default. |
| Username/Password | Enter the user name/password of the device you need. |
| Channel No. | If the target device 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. |

3) Click **OK**.

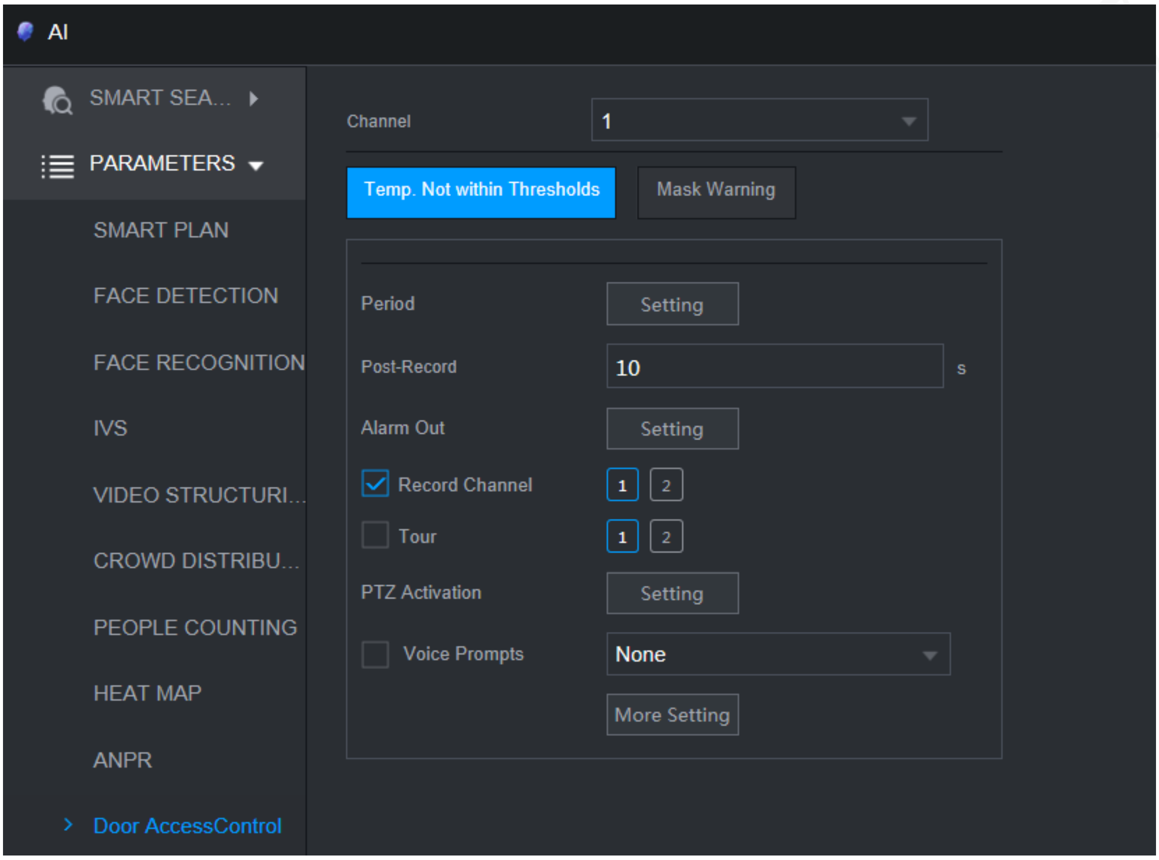
## 6.2.2 Enabling Temperature and Mask Monitoring

Step 1 Log in to NVR, and then select **AI > Parameters > Door Access Control**.

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

Step 3 Click **Temp.Not within Thresholds** or **Mask Warning**.

Figure 6-12 Set temperature or mask monitoring



Channel 1

Period Setting

Post-Record 10 s

Alarm Out Setting

☑ Record Channel 1 2

□ Tour 1 2

PTZ Activation Setting

□ Voice Prompts None

Step 4 Set the following parameters.

Table 6-4 Temperature monitoring parameters

| Parameter | Description |
|---|---|
| Period | Click **Settting** to set the temperature monitoring schedule. |
| Post-Record | Specify how many seconds you want the device to keep recording after an event is detected. |
| Record Channel | Select Channel 1 or 2 to record video. |
| Voice Prompt | Set the voice promt for an temperature alarm. |
| More Setting | Click **More Setting**, and then you can select the alarm-linked actions, such as buzzer, alarm upload, and email.<br>To enable **Send Email**, you need to go to **MANAGEMENT > NETWORK > EMAIL** and set email parameters in advance. |

## 6.2.3 (Optional) Enabling Fahrenheit

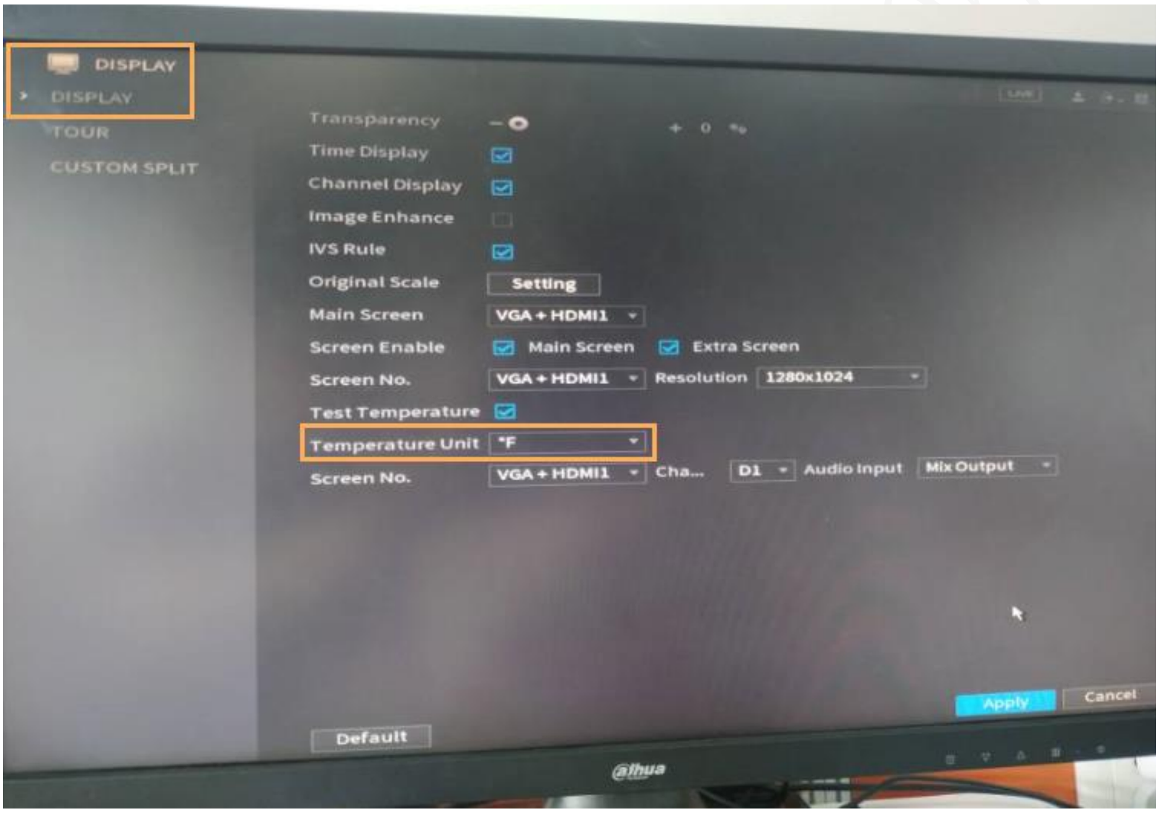
If you use Fahrenheit, you need to enable Fahrenheit both on the face recognition terminal and the NVR.

For how to enable Fahrenheit on the face recognition terminal, see "6.1.3 Configuring Face Recognition Parameters."

Step 1 Log in to the local interface of NVR.

Step 2 On the **Display** interface, select **°F** from the drop-down list of **Temperature Unit**.

Figure 6-13 Set Fahrenheit



Transparency
Time Display ☑
Channel Display ☑
Image Enhance □
IVS Rule ☑
Original Scale Setting
Main Screen VGA+HDMI1
Screen Enable ☑ Main Screen ☑ Extra Screen
Screen No. VGA+HDMI1 Resolution 1280x1024
Test Temperature ☑
Temperature Unit °F
Screen No. VGA+HDMI1 Cha... D1 Audio Input Mix Output

Step 3 Click **Apply**.

## 6.2.4 Commissioning

### Preparation

- Face recognition terminal is correctly installed and connected.
- Unlock mode, face database, face recognition parameters are correctly configured on the face recognition terminal.
- Face recognition terminal is added to NVR.
- Temperature and mask monitoring are enabled on NVR.

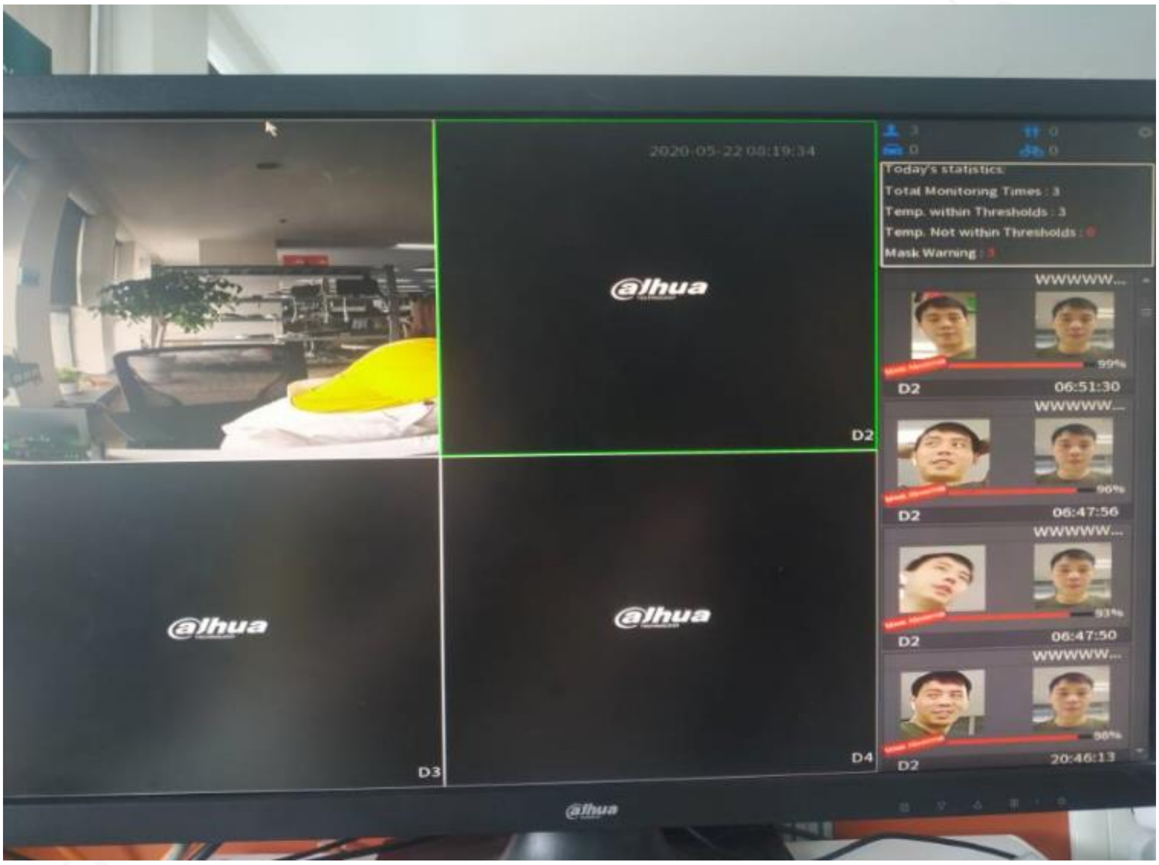
## Objectives

NVR displays the results of face recognition, temperature measurement and mask detection in real-time.

## Procedure

On the local interface of NVR, go to the **Live** interface, and select the face recognition terminal channel. Stand in front of the terminal, and then check whether the NVR shows body temperature and mouth mask monitoring results.

Figure 6-14 Live monitoring on NVR



Today's statistics:
Total Monitoring Times : 3
Temp. within Thresholds : 3
Temp. Not within Thresholds : 0
Mask Warning : 3

# 6.3 Configuring Express

After installing and activating Express, you need to add face recognition terminal, set recording plan and storage space. Skip this chapter if you do not have Express in your product combination.

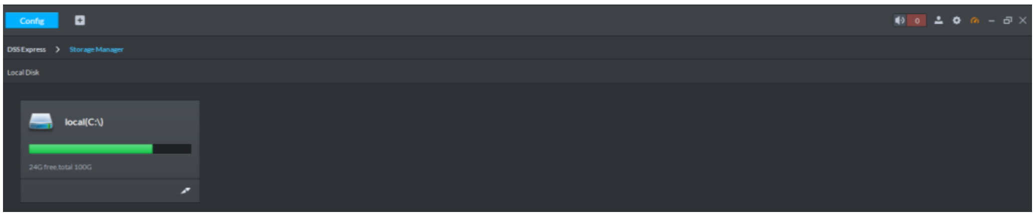
## 6.3.1 Configuring Storage Space on Express

Configure the disks in the server of Express to store video and pictures. Configure at least one disk for picture storage.

Step 1 Log in to Express Client.

Step 2 Select **Config > Storage**.

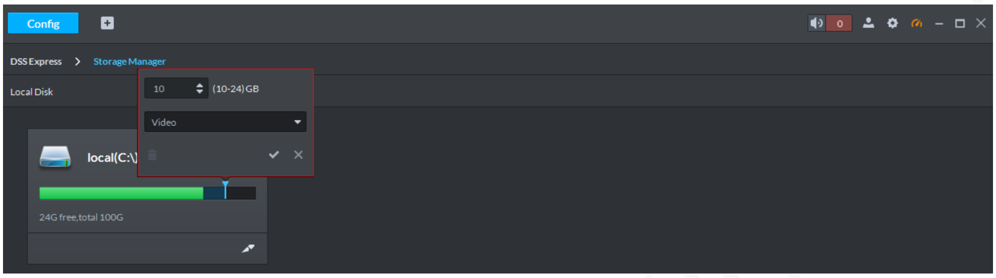
Figure 6-15 Storage manager



Step 3 Click ✎.

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

Figure 6-16 Create storage space



Step 4 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.

Figure 6-17 Disk status change

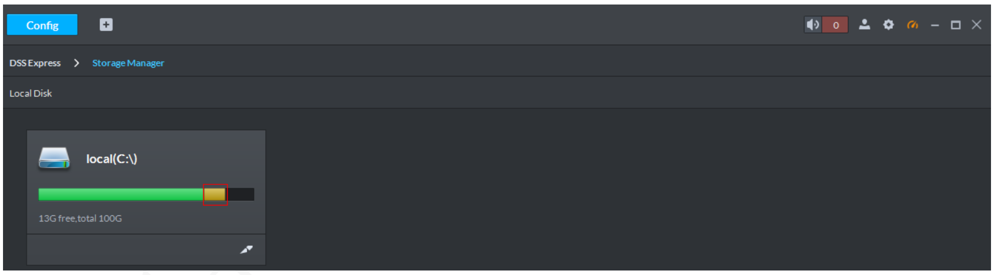
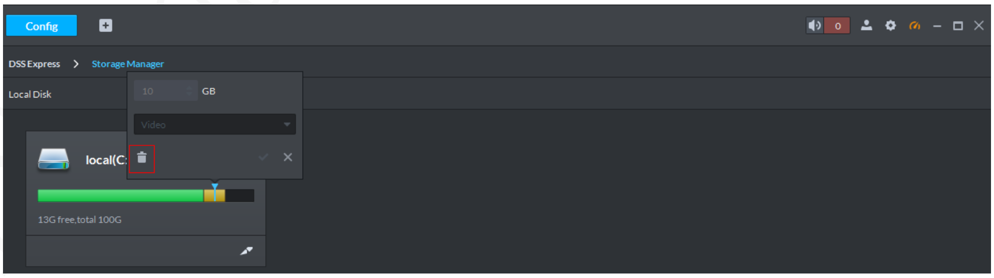


Figure 6-18 Delete exclusive storage space



## 6.3.2 Adding Face Recognition Terminal to Express

Add the face recognition terminals to Express so that you can view live or recorded videos, search for access and temperature measurement records, and check alarms on Express client. You can add by entering device information, or search the network for online devices to quickly add them.

### 6.3.2.1 Adding by Search

Select this method when the device you are going to add can be detected on Express, thus you do not need to enter the device parameters.

If you have multiple devices to add, and they have the same username and password, you can select this method to add them in batches.

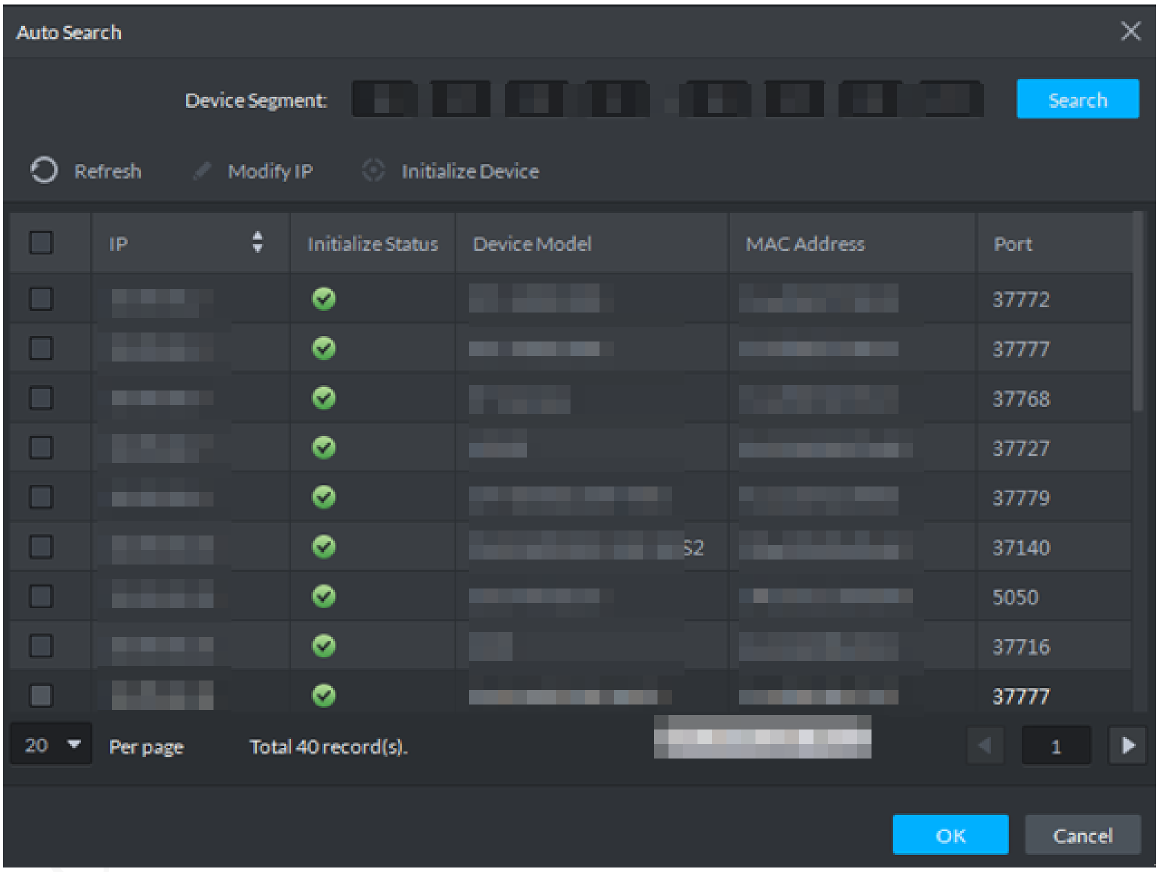
Step 1 Log in to Express Client.

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

Step 3 Click **Auto Search**.

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

Figure 6-19 Auto search



Device Segment: [redacted]

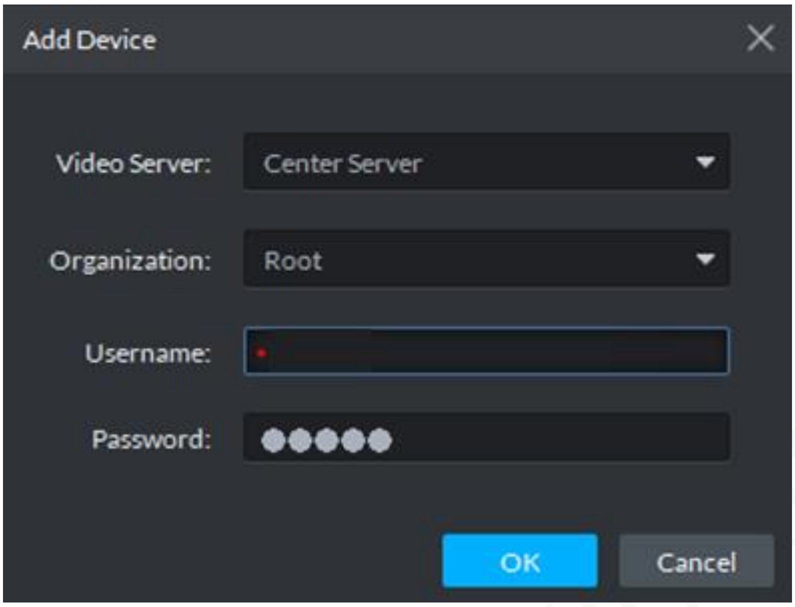
| ☐ | IP | Initialize Status | Device Model | MAC Address | Port |
|---|---|---|---|---|---|
| ☐ | [redacted] | ✓ | [redacted] | [redacted] | 37772 |
| ☐ | [redacted] | ✓ | [redacted] | [redacted] | 37777 |
| ☐ | [redacted] | ✓ | [redacted] | [redacted] | 37768 |
| ☐ | [redacted] | ✓ | [redacted] | [redacted] | 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

Step 4 Enter the IP range (start IP and end IP), and then click **Search**.

Step 5 Select the device to be added, click **OK**.

Figure 6-20 Add Device



Video Server: Center Server

Organization: Root

Username: *

Password: ●●●●●

Step 6 Enter login username and password, and then click **OK**.

### 6.3.2.2 Adding Manually

Select this method when you add a single device, or the username and password of the devices are different, or the added device is not in the same segment.

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

Step 2 Click **Add**.

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 6-5 Parameter description

| Parameter | Description |
|---|---|
| Device Category | Select **Access Control**. |
| Register Mode | Support registration by following method:<br>● IP address<br>Add device to platform by adding device IP.<br>● Serial number (Device with P2P function)<br>If device supports P2P function, then you can add device to platform by adding device serial number.<br>● ONVIF<br>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:<br>● Pull<br>Decoder extracts stream from platform by url address, the decode mode of device is pull.<br>● Direct<br>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.<br>● Push<br>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.

### 6.3.3 Modifying Channel Number and Features

After adding the terminal to Express, you need to modify the number and features of video channels under this terminal.

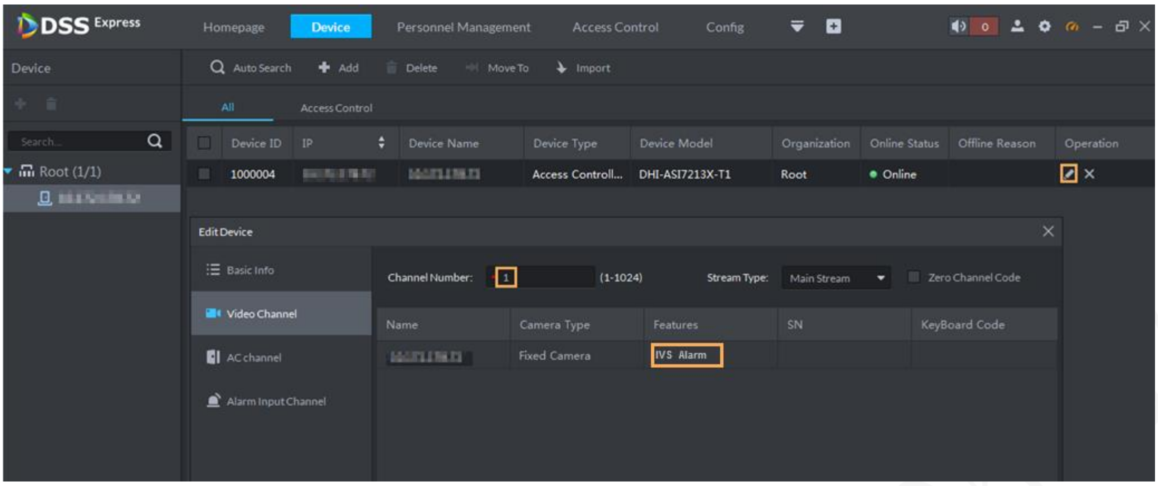
Step 1 Log in to Express Client.

Step 2 On the **Homepage**, click **Device** at the lower-left corner.

Step 3 Select the face recognition terminal from the device tree, and then click ✎

Step 4 On the **Edit Device** interface, click the **Video Channel** tab.

Step 5 Modify the value in the **Channel Number** box from 0 to 1, select **IVS Alarm** from the **Features** drop-down list, and then the video channel of the face recognition terminal is added to Express.



| Device ID | IP | Device Name | Device Type | Device Model | Organization | Online Status | Offline Reason | Operation |
|---|---|---|---|---|---|---|---|---|
| 1000004 | | | Access Controll... | DHI-ASI7213X-T1 | Root | Online | | |

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

| Name | Camera Type | Features | SN | KeyBoard Code |
|---|---|---|---|---|
| | Fixed Camera | IVS Alarm | | |

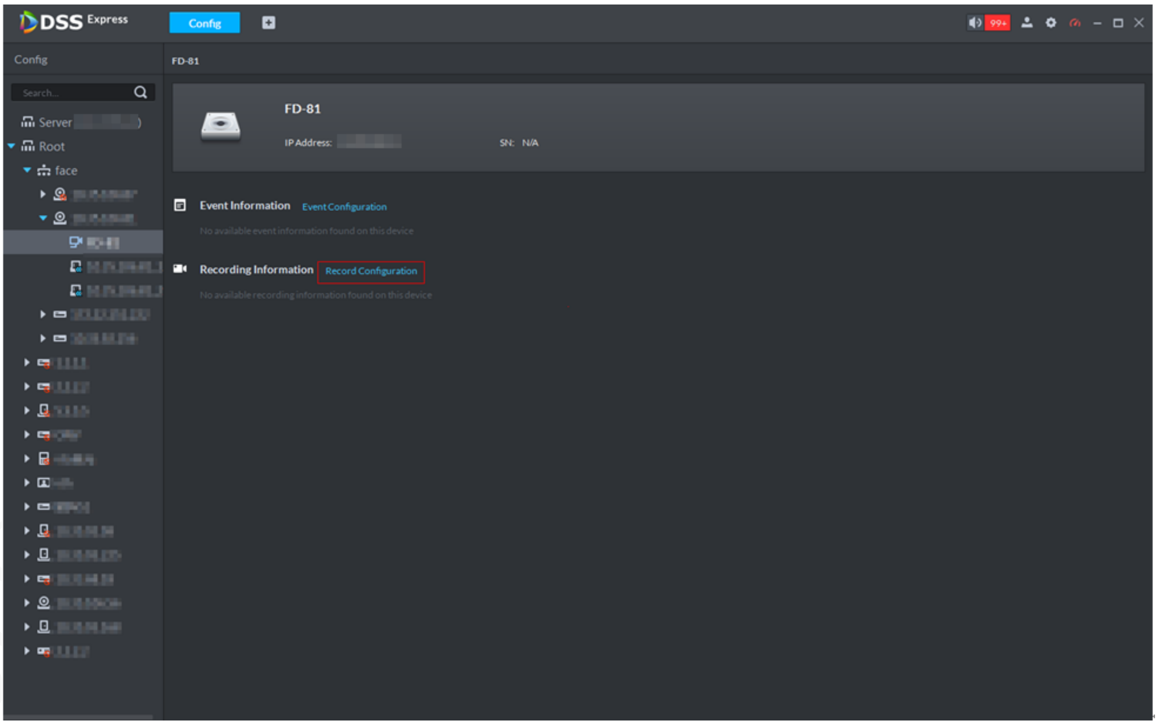
## 6.3.4 Configuring Video Recording Plan on Express

Step 1 Log in to Express Client.

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

Step 3 From the device tree on the left, select camera channel of the face recognition terminal, and then click **Record Configuration**.

Figure 6-21 Enter record configuration interface



FD-81

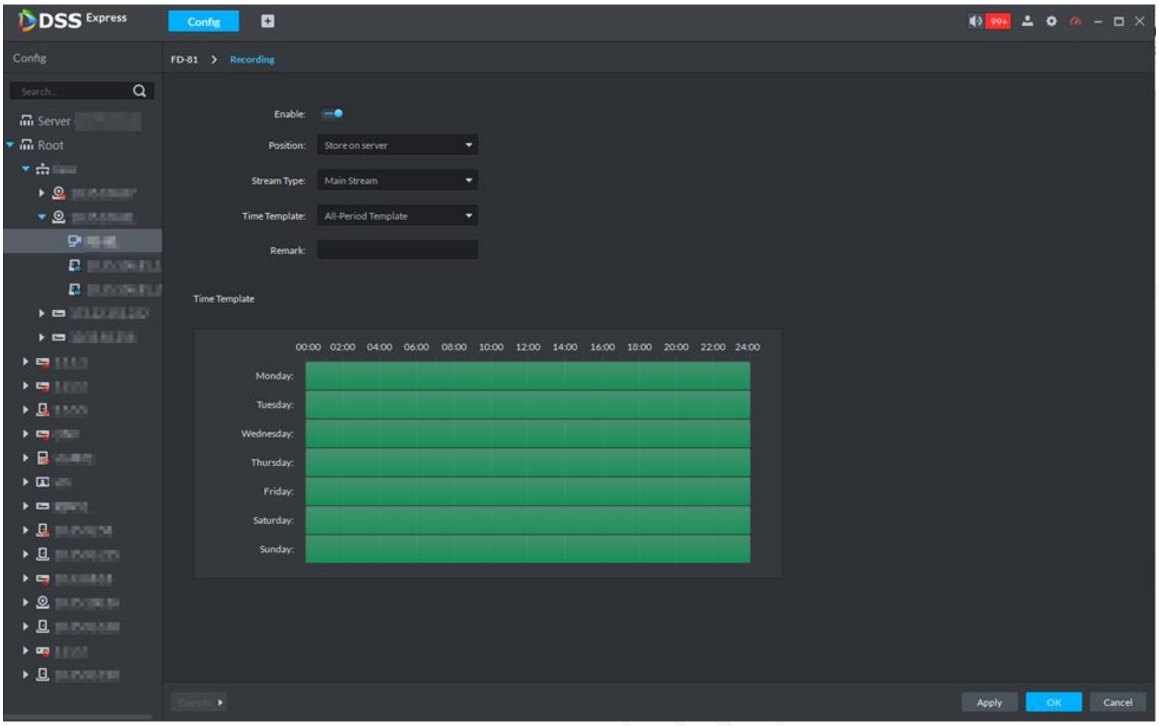
IP Address:

SN: N/A

No available event information found on this device

No available recording information found on this device

Figure 6-22 Record



Enable:
Position: Store on server
Stream Type: Main Stream
Time Template: All-Period Template
Remark:

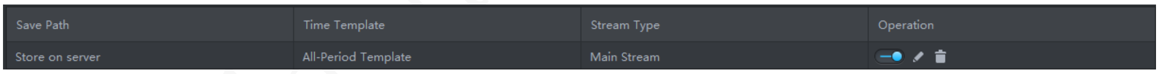
Step 4 Click .

The icon is switched to , enable record plan.

Step 5 Set Position, Stream Type and Time Template. Select Store on Server for Position.

Step 6 Click **OK**.

Figure 6-23 Record info



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

## 6.3.5 Configuring People Information

Register people information such as face image and card No. into the system and assign access permissions, so that the system can identify people and let go accordingly.

You can add people information one by one or in batches. If you have many people to add, add them in batches.

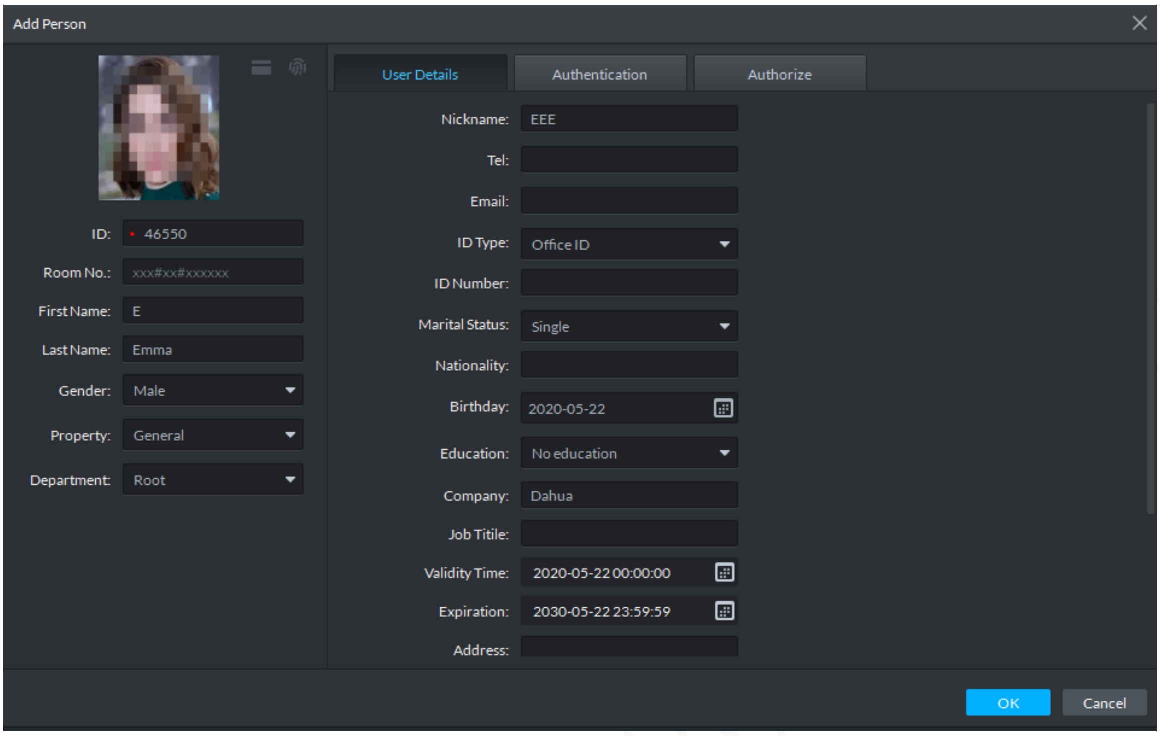
- One by one

Step 1 Log in to Express Client.

Step 2 Select **Personnel Management**, and then click **Add**.

Step 3 Click the **User Details** tab to configure person information.

Figure 6-24 Add a person



ID: 46550
Room No.: xxx#xx#xxxxxx
First Name: E
Last Name: Emma
Gender: Male
Property: General
Department: Root

Nickname: EEE
Tel:
Email:
ID Type: Office ID
ID Number:
Marital Status: Single
Nationality:
Birthday: 2020-05-22
Education: No education
Company: Dahua
Job Titile:
Validity Time: 2020-05-22 00:00:00
Expiration: 2030-05-22 23:59:59
Address:

1) Move the mouse cursor to the picture section, and then click **Upload**. Follow the instructions on the interface to upload a picture. If the PC comes with a camera, click **Snapshot** to take a face snapshot and upload it.

2) Fill in personnel information as necessary. ID is required, and others are optional.

Person ID shall be the same on the platform and access control devices; otherwise person data could be wrong.

Step 4 Click the **Authentication** tab

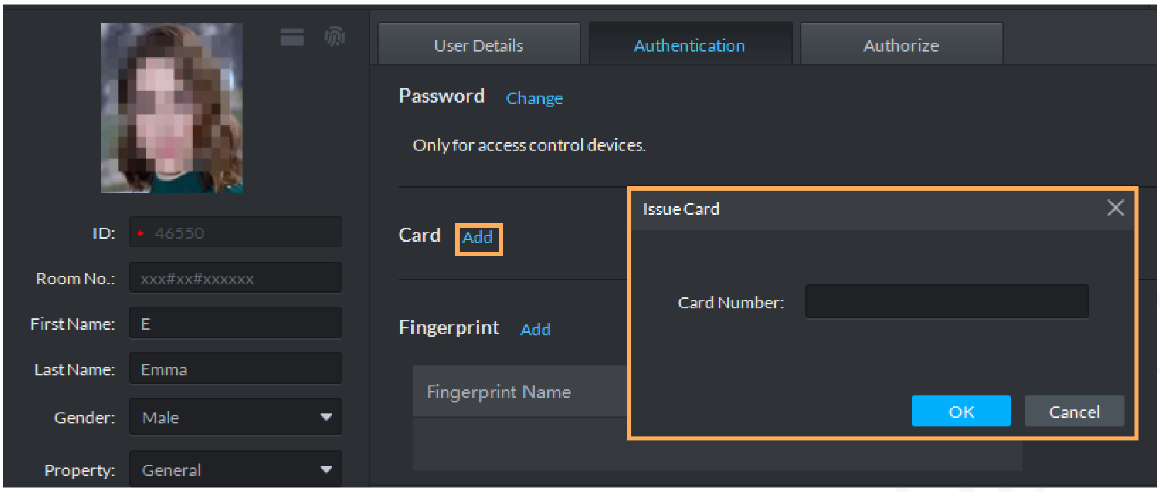
Step 5 Add a card.

One person can have up to 5 cards. There are two ways to issue cards: by entering card No. and by card reader. Card No. can contain 8 or 16 numbers. 16-digit card No. is only available with the second-generation access control devices. When a card No. is less than 8 or 16 numbers, the system will automatically add zeros prior to the No. to make it 8 or 16 digits. For example, if the provided No. is 8004, it will become 00008004; if the provided No. is 1000056821, it will become 0000001000056821.

- By entering card No.

1) Click **Add** next to **Card**.

Figure 6-25 Issue card by entering card No.



ID: • 46550

Room No.: xxx#xx#xxxxxx

First Name: E

Last Name: Emma

Gender: Male

Property: General

Password Change

Only for access control devices.

Card Add

Fingerprint Add

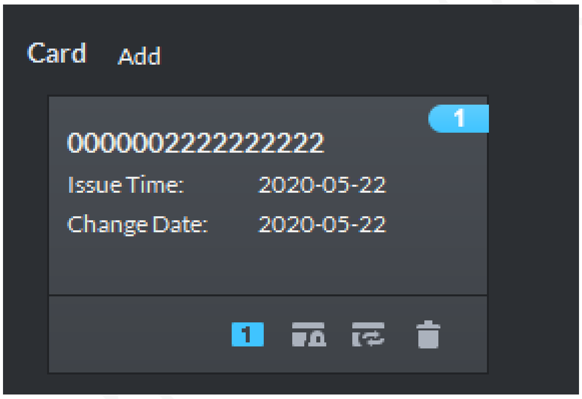
Issue Card

Card Number:

2) Enter card number and click **OK**.

The card is added.

Figure 6-26 Added card



Card Add

0000002222222222

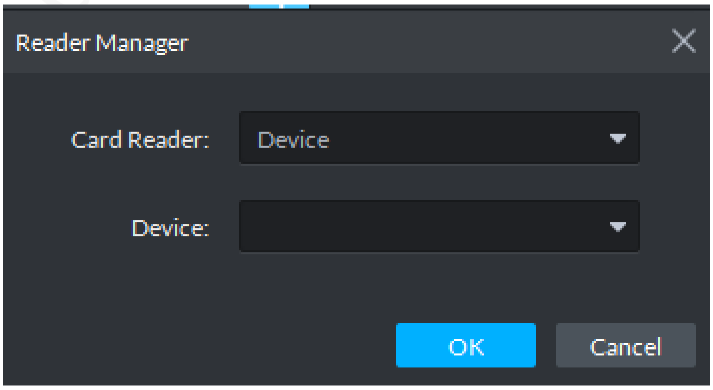
Issue Time: 2020-05-22

Change Date: 2020-05-22

- By card reader

1) Click ⚙.

Figure 6-27 Issue card by card reader



Reader Manager

Card Reader: Device

Device:

2) Select **Card Issuer** or **Device**, and then click **OK**.

If you select **Card Issuer**, make sure you have connected a card issuer.

Swipe card on the card reader or device, and then the card is added.

Step 6 Add face images.

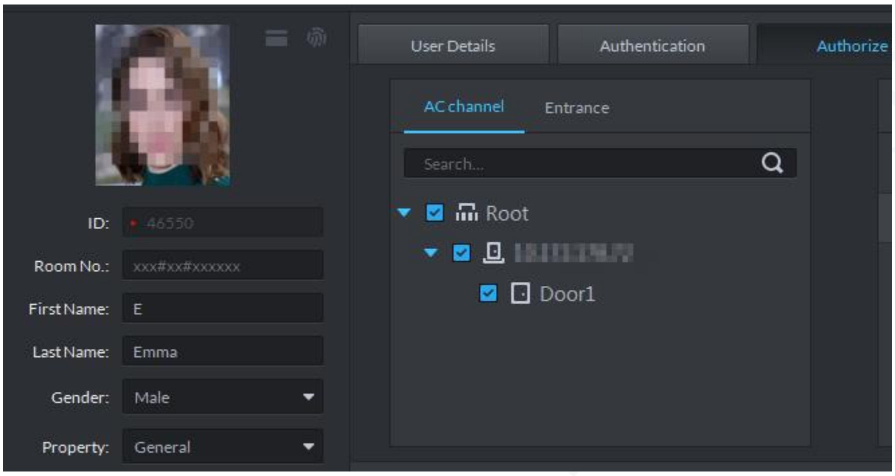
Click **Add** next **Face Comparison**, and then select a face image.

You can click **Add** again to upload one more face image for the person, a side face image for example, so as to increase recognition accuracy,

Step 7 Click the **Authorize** tab.

Select the accessible doors for this person.

Figure 6-28 Authorize



ID: 46550

Room No.: xxx#xx#xxxxxx

First Name: E

Last Name: Emma

Gender: Male

Property: General

Step 8 Click **OK**.

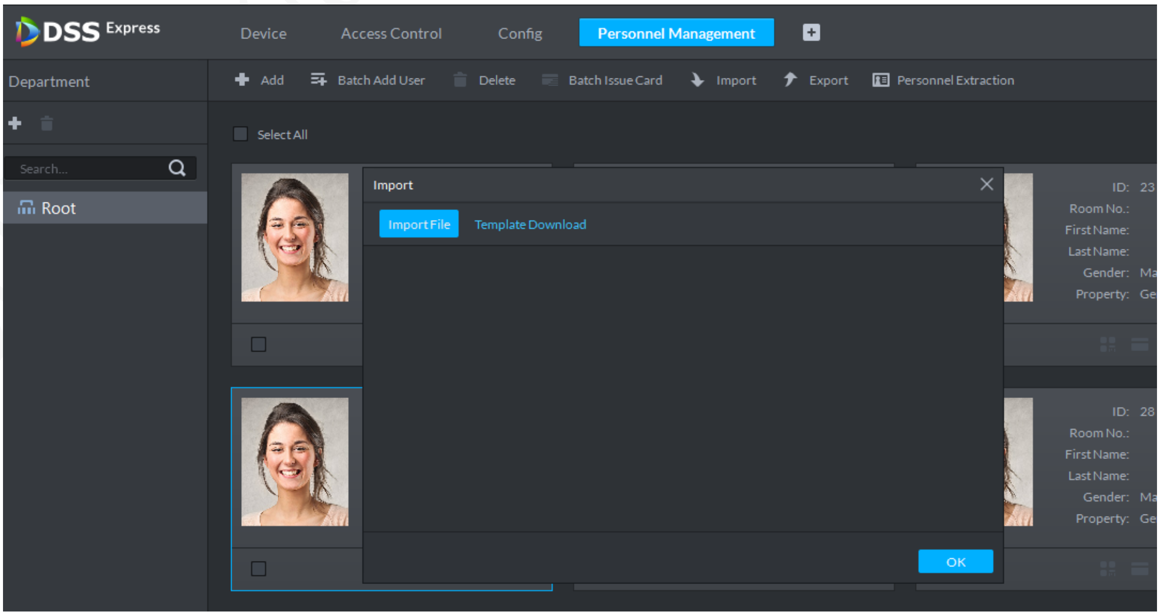
- In batches

Step 1 Log in to Express Client.

Step 2 Add people info.

1) Select **Personnel Management**, click Import **> Template Download**, and then save the template locally.

Figure 6-29 Download template



2) Unzip the template, provide the face images, name them, and then fill people info in the template. When filling the template, confirm to the rules as descripted in the file.

3) Zip the file again.

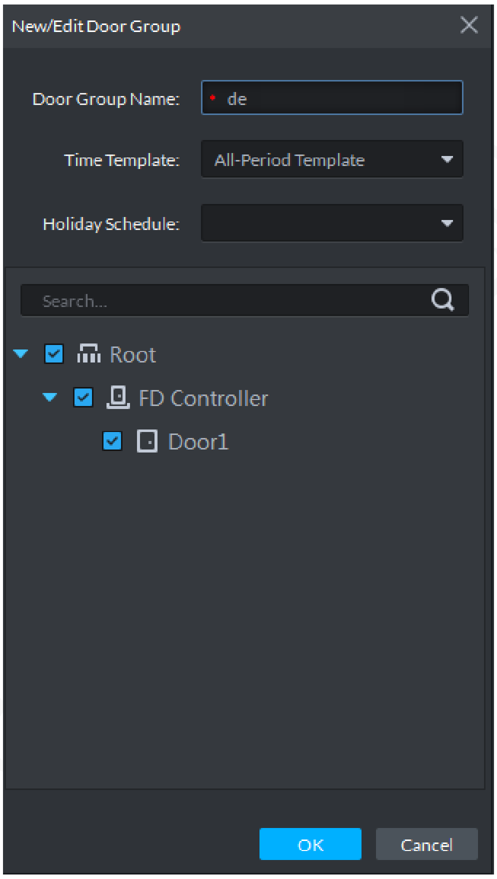
4) Go back to Express, and then on the **Import** interface (see Figure 6-29), click **Import** File to upload the ZIP file.

Step 3 Add door groups.

1) On the **Homepage**, select **Access Control**, and then click .

2) Click **Door Group**, and then click **Add** to add a door group.

Figure 6-30 Add a door group



New/Edit Door Group

Door Group Name: * de

Time Template: All-Period Template

Holiday Schedule:

Search...

☑ Root

☑ FD Controller

☑ Door1

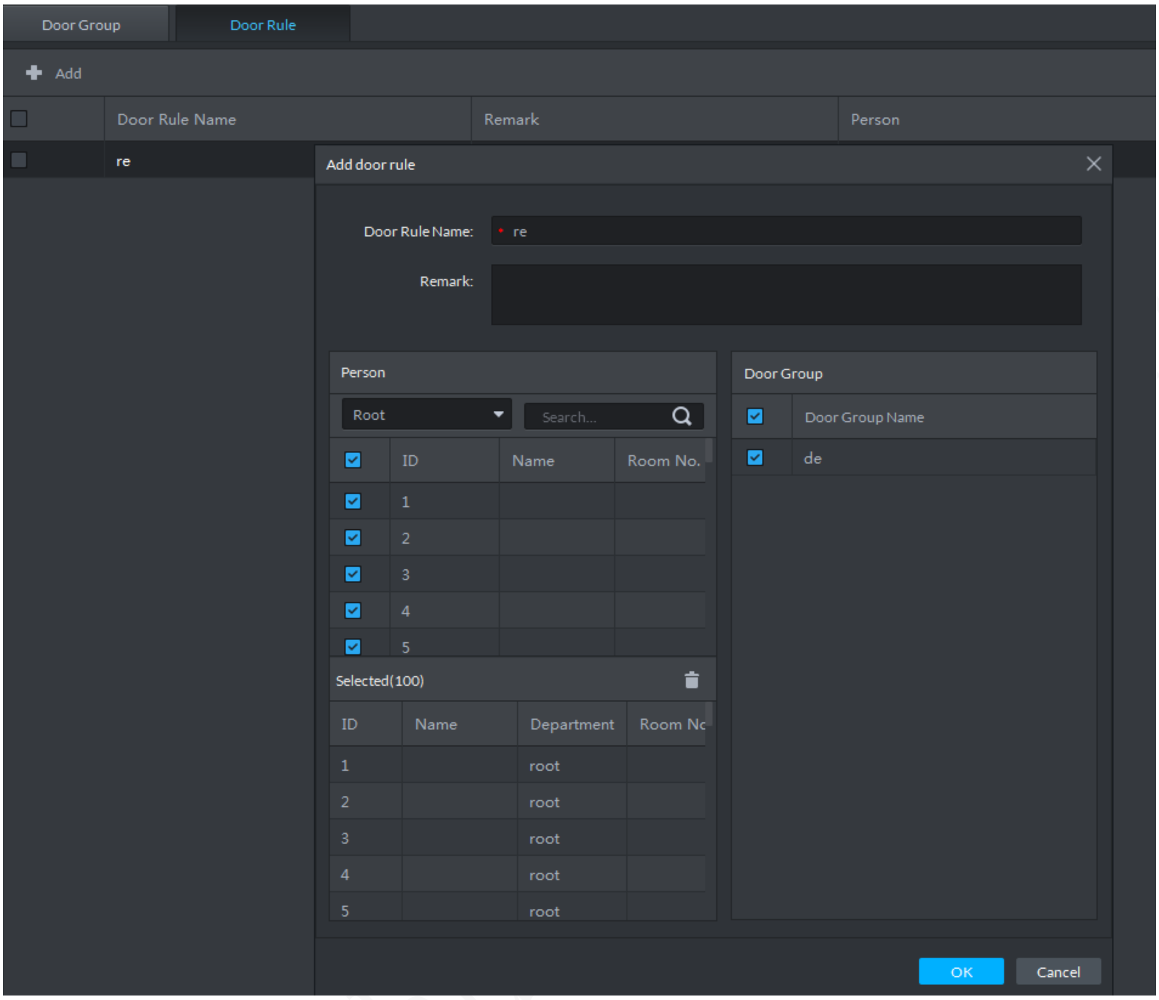
3) Click **OK**.

Step 4 Assign door groups to people.

This operation is to assign door groups to the selected people so that they can have access to the doors.

1) Click the **Door Rule** tab, and then click **Add** to add a door rule.

Figure 6-31 Add a door rule



| ☐ | Door Rule Name | Remark | Person |
|---|---|---|---|
| ☐ | re | | |

Door Rule Name: re

Remark:

| ☑ | ID | Name | Room No. |
|---|---|---|---|
| ☑ | 1 | | |
| ☑ | 2 | | |
| ☑ | 3 | | |
| ☑ | 4 | | |
| ☑ | 5 | | |

Selected(100)

| ID | Name | Department | Room Nc |
|---|---|---|---|
| 1 | | root | |
| 2 | | root | |
| 3 | | root | |
| 4 | | root | |
| 5 | | root | |

| ☑ | Door Group Name |
|---|---|
| ☑ | de |

2) Name the rule, select the check boxes of the people you need to select, and then select the door groups you want to assign to them.

3) Click **OK**.

The selected people then have the right of access through the selected doors.

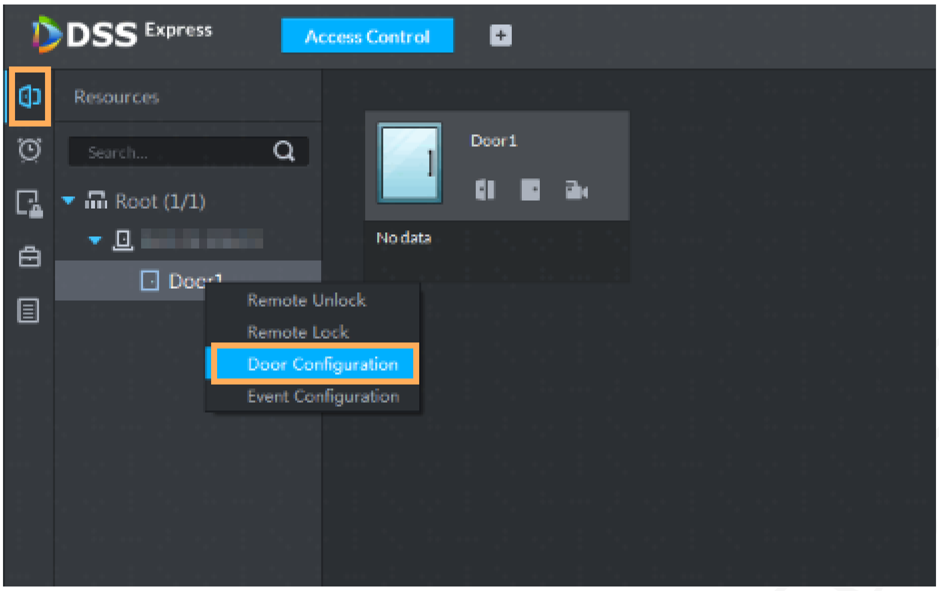
## 6.3.6 Configuring Door Unlock Method

Set door unlock method, such as face recognition or face recognition + card.

Step 1 Log in to the Express Client.

Step 2 Select **Access Control >** .

Step 3 Right-click on the door channel of the face recognition terminal, and then click Door Configuration.

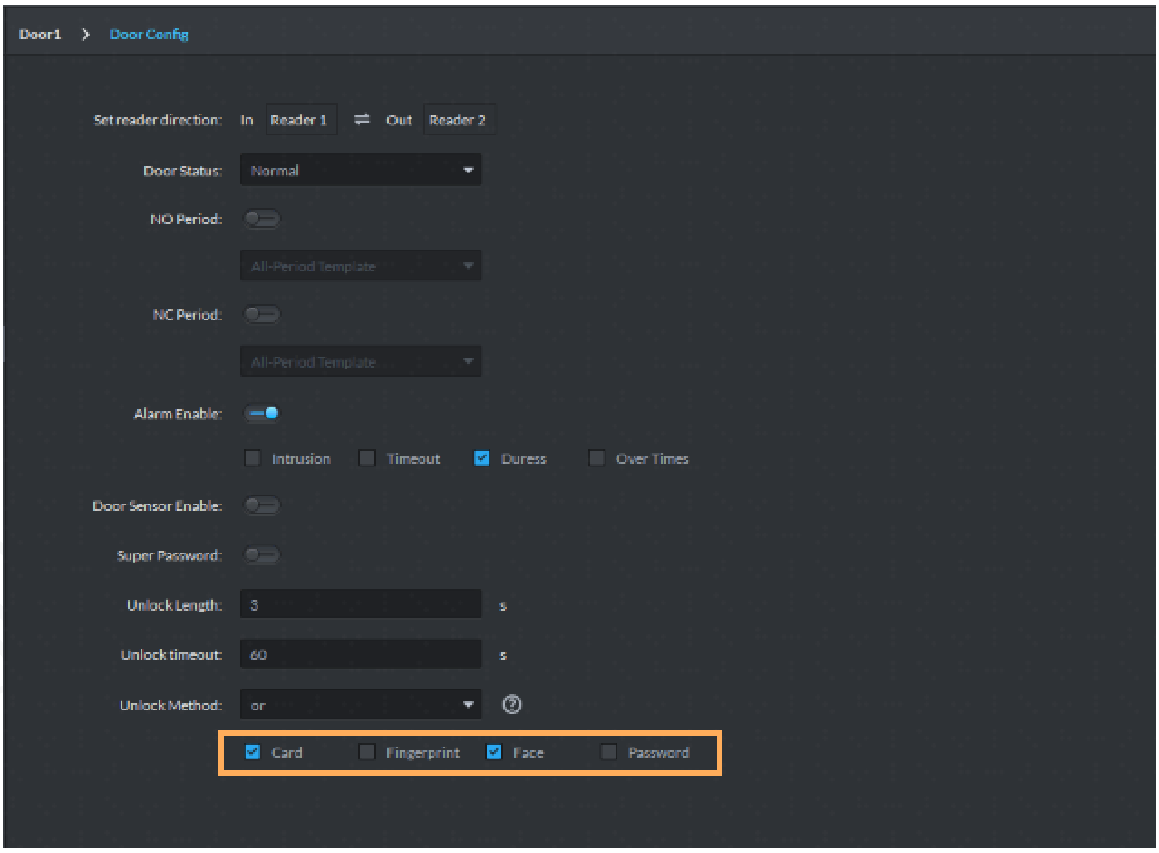


Step 4 Select **or** or **and** from the **Unlock Method** drop-down list.

- Select **or**: The door can be opened by any of the selected methods.
- Select **and**: The door opens after all the selected methods are performed and passed.

Step 5 Select the method(s) you need. In this solution, you need to select **Face**, or **Face and Card**. The Face method is required, and others are optional.

Figure 6-32 Set unlock method(s)


Door1 > Door Config

Set reader direction: In Reader 1 ⇄ Out Reader 2

Door Status: Normal

NO Period: ○

All-Period Template

NC Period: ○

All-Period Template

Alarm Enable: ●

□ Intrusion □ Timeout ☑ Duress □ Over Times

Door Sensor Enable: ○

Super Password: ○

Unlock Length: 3 s

Unlock timeout: 60 s

Unlock Method: or

☑ Card □ Fingerprint ☑ Face □ Password

Step 6 Click **Apply**.

Configuring

## 6.3.7 Configuring Temperature and Mask Alarms

Configure temperature and mask alarms. Otherwise you cannot receive the alarms on Express.

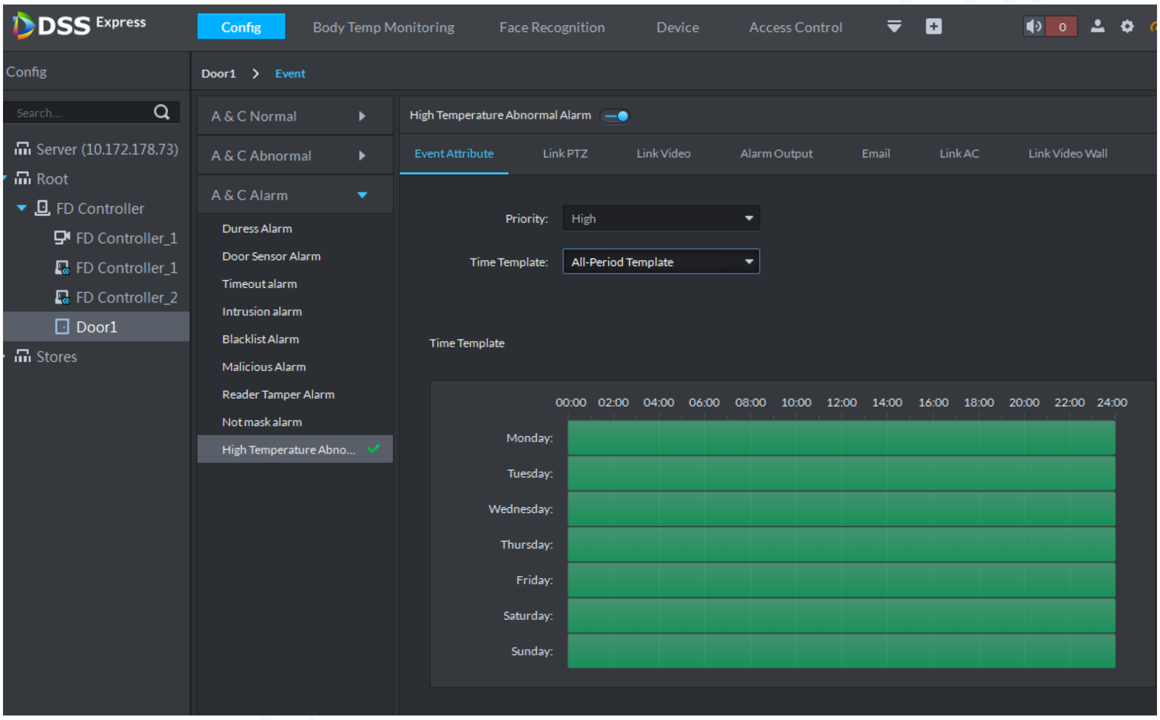
Step 1 On the **Homepage** of Express, click **Config**.

Step 2 Select the Door channel under the face recognition terminal, and then click **Event Configuration**.

Step 3 Click **A & C Alarm**, click **High Temperature Abnormal Alarm** or **Not mask alarm**, and then click ○ to enable it. ● indicates that the alarm is enabled.

Step 4 Set alarm priority, and then select a template. The alarm is received and reported during the period of the template.

Figure 6-33 Set alarms



Priority: High

Time Template: All-Period Template

Step 5 Set linked actions.

- Click **Link Video**, select the face recognition terminal from the device list, and then select the check boxes next to **After alarm is triggered, camera snapshot** and **When alarm is triggered, open camera on client**.
- Click **Email**, and then set email parameters.

Step 6 Click **OK**.

## 6.3.8 Commissioning

### 6.3.8.1 Live Monitoring

#### Preparation

- Face recognition terminal is correctly installed and connected.
- Face recognition terminal is added to Express.
- The video channel number of the face recognition terminal is modified, and the feature of the video channel is set to IVS alarm.

#### Objectives

Express displays face recognition, temperature monitoring and mask detection results in real time.

#### Procedure

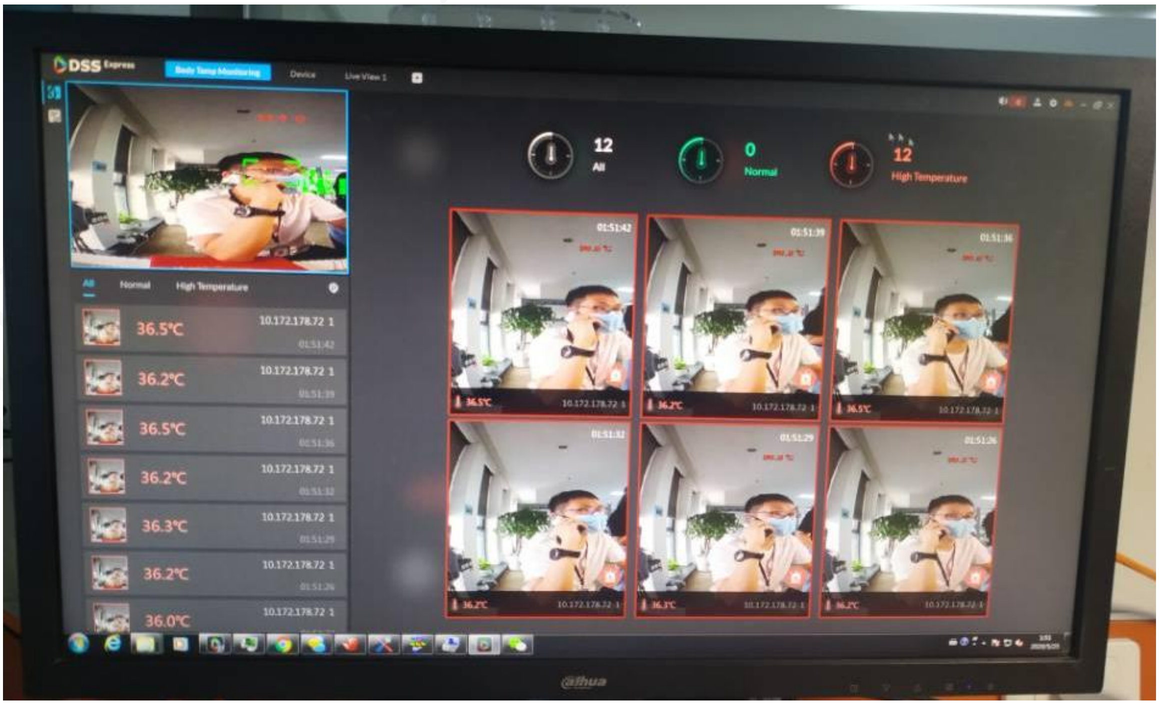
Step 1 Log in to the Express Client

Step 2 Select **Body Temp Monitoring**.

The results are displayed in real time.

You can click ◉ to change device channels.

Figure 6-34 Live monitoring



### 6.3.8.2 Viewing Access Control Records (with Temperature and Mask-wearing Info)

## Preparation

- Face recognition terminal and turnstile are correctly installed and connected.
- Face database and face recognition parameters are correctly configured on the face recognition terminal.
- Face recognition terminal is added to Express.
- The video channel number of the face recognition terminal is modified, and the feature of the video channel is set to IVS alarm.
- Storage space and recording plan are configured on Express.
- People information such as face, card and door permission is configured.
- Door unlock method is configured.

## Objectives

Express displays face recognition, temperature measurement and mask detection results in the access control records.

## Procedure

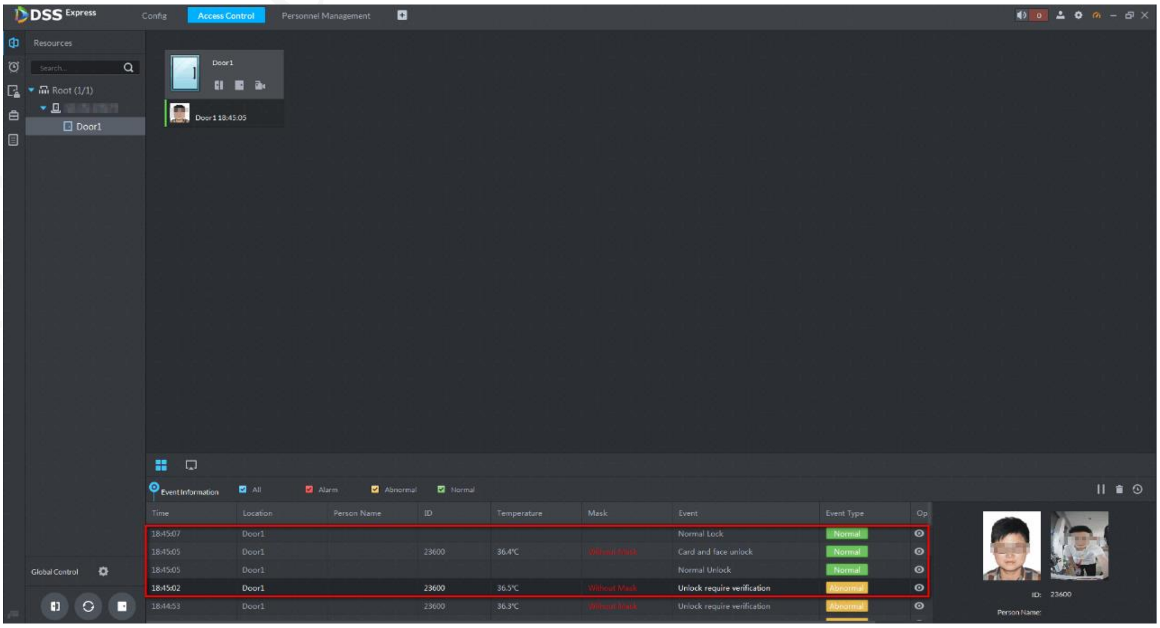
Step 1 Log in to the Express Client

Step 2 Select **Access Control**.

Step 3 Click ◫ to check the real-time records or ▤ to search for history records.

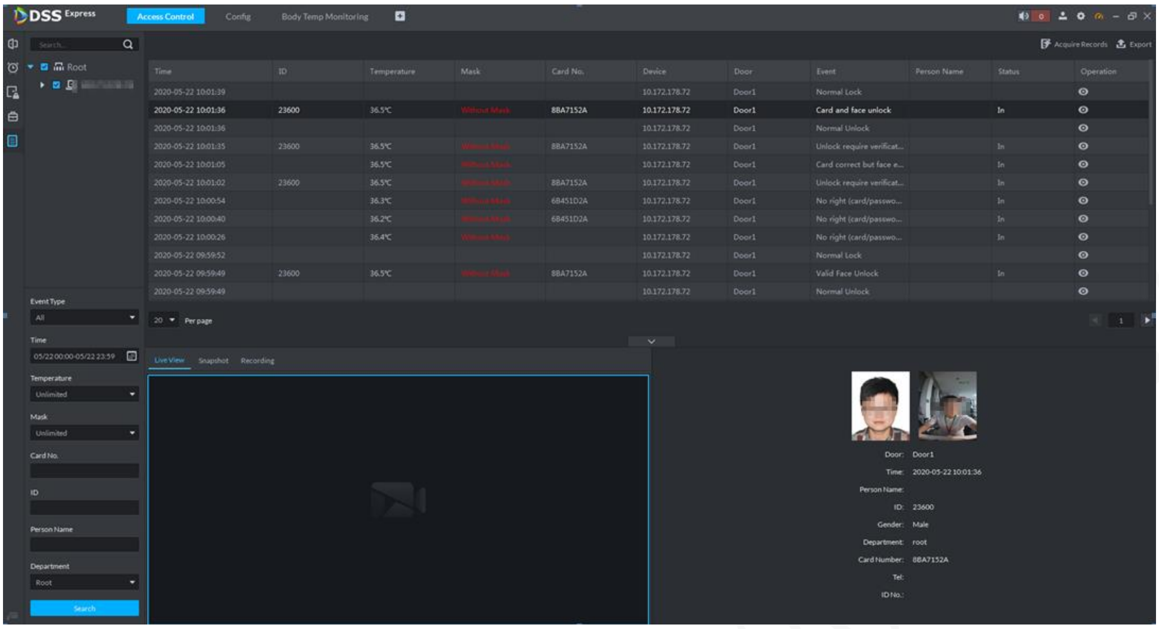
Check whether the access control records show face recognition results, temperature measurement results and mask-wearing info.

Figure 6-35 Real-time access control records



| Time | Location | Person Name | ID | Temperature | Mask | Event | Event Type | Op |
|---|---|---|---|---|---|---|---|---|
| 18:45:07 | Door1 | | | | | Normal Lock | Normal | |
| 18:45:05 | Door1 | | 23600 | 36.4℃ | Without Mask | Card and face unlock | Normal | |
| 18:45:05 | Door1 | | | | | Normal Unlock | Normal | |
| 18:45:02 | Door1 | | 23600 | 36.5℃ | Without Mask | Unlock require verification | Abnormal | |
| 18:44:53 | Door1 | | 23600 | 36.3℃ | Without Mask | Unlock require verification | Abnormal | |

Figure 6-36 History access control records



| Time | ID | Temperature | Mask | Card No. | Device | Door | Event | Person Name | Status | Operation |
|---|---|---|---|---|---|---|---|---|---|---|
| 2020-05-22 10:01:39 | | | | | 10.172.178.72 | Door1 | Normal Lock | | | 👁 |
| 2020-05-22 10:01:36 | 23600 | 36.5℃ | Without Mask | 8BA7152A | 10.172.178.72 | Door1 | Card and face unlock | | In | 👁 |
| 2020-05-22 10:01:36 | | | | | 10.172.178.72 | Door1 | Normal Unlock | | | 👁 |
| 2020-05-22 10:01:35 | 23600 | 36.5℃ | Without Mask | 8BA7152A | 10.172.178.72 | Door1 | Unlock require verificat... | | In | 👁 |
| 2020-05-22 10:01:05 | | 36.5℃ | Without Mask | | 10.172.178.72 | Door1 | Card correct but face e... | | In | 👁 |
| 2020-05-22 10:01:02 | 23600 | 36.5℃ | Without Mask | 8BA7152A | 10.172.178.72 | Door1 | Unlock require verificat... | | In | 👁 |
| 2020-05-22 10:00:54 | | 36.3℃ | Without Mask | 6B451D2A | 10.172.178.72 | Door1 | No right (card/passwo... | | In | 👁 |
| 2020-05-22 10:00:40 | | 36.2℃ | Without Mask | 6B451D2A | 10.172.178.72 | Door1 | No right (card/passwo... | | In | 👁 |
| 2020-05-22 10:00:26 | | 36.4℃ | Without Mask | | 10.172.178.72 | Door1 | No right (card/passwo... | | In | 👁 |
| 2020-05-22 09:59:52 | | | | | 10.172.178.72 | Door1 | Normal Lock | | | 👁 |
| 2020-05-22 09:59:49 | 23600 | 36.5℃ | Without Mask | 8BA7152A | 10.172.178.72 | Door1 | Valid Face Unlock | | In | 👁 |
| 2020-05-22 09:59:49 | | | | | 10.172.178.72 | Door1 | Normal Unlock | | | 👁 |

20 Per page

1

Event Type: All

Time: 05/22 00:00-05/22 23:59

Temperature: Unlimited

Mask: Unlimited

Card No.:

ID:

Person Name:

Department: Root

Search

Door: Door1

Time: 2020-05-22 10:01:36

Person Name:

ID: 23600

Gender: Male

Department: root

Card Number: 8BA7152A

Tel:

ID No.:

# 6.4 Configuring DMSS

DMSS is a mobile App that can manage your system and provide video monitoring wherever you are. Skip this chapter if you do not use DMSS.

- Make sure that DMSS can visit the face recognition terminal. For example, if the face recognition terminal is in the LAN, you can set wireless LAN on the router for DMSS; if DMSS can only connect 3G/4G, you need to connect the face recognition terminal to the public network. For details, contact your IT engineer.
- You cannot create face database on NVR. For the "face recognition terminal – NVR" solution, you need to create face database on the face recognition terminal. For details, see "6.1.2 Creating Face Database."

## 6.4.1 Adding Face Recognition Terminal to DMSS

There are the following three ways to add the face recognition terminal to DMSS.

### 6.4.1.1 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**.

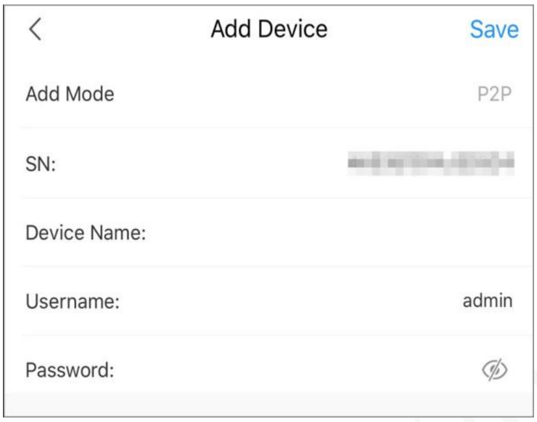
Step 2 Scan device QR code, or manually enter device SN, and then the system will identify the device type automatically. If the device type cannot be automatically identified by the system, you need to select the device type.

If you scan QR code to add face recognition terminal, perform the following steps.

1) Log in to the web interface of the face recognition terminal, and then select **Network Setting > P2P**.
2) Select **Enable** to enable P2P function.
3) Click **OK**.

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

Figure 6-37 Add face recognition terminal (SN/scan)



Add Mode: P2P

SN: [redacted]

Device Name:

Username: admin

Password:

## 6.4.1.2 Adding by IP/Domain

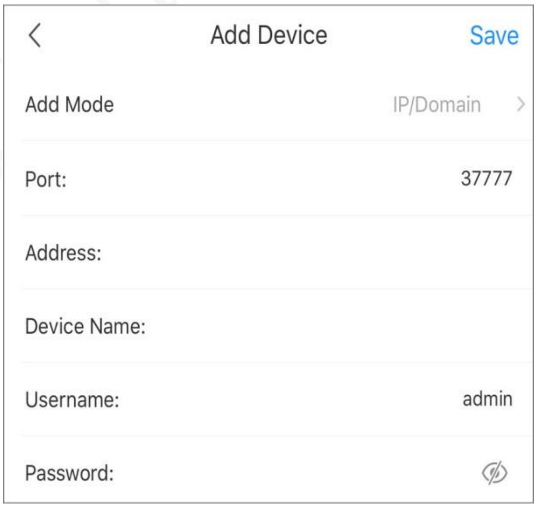
You can add devices by entering IP of the device or specific domain. This section takes entering device IP as an example.

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 6-38 Add face recognition terminal (IP/domain)



Add Mode: IP/Domain

Port: 37777

Address:

Device Name:

Username: admin

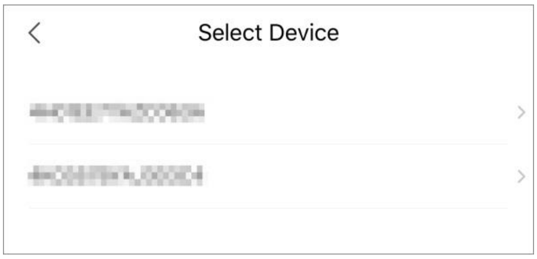
Password:

## 6.4.1.3 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 6-39 Select device SN



Select Device

[redacted]

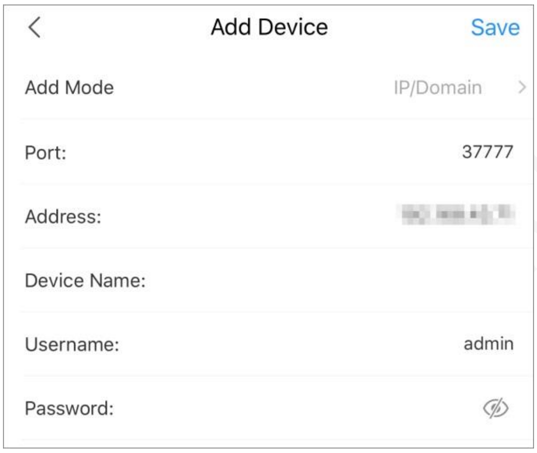
[redacted]

Step 2 Tap the device SN as needed.

The device type interface is displayed.

Step 3 Select the device type.

Figure 6-40 Add face recognition terminal (search online)



Add Mode: IP/Domain

Port: 37777

Address: [redacted]

Device Name:

Username: admin

Password:

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

## 6.4.2 Configuring Video/Image Storage

Store video/image on SD card or DMSS cloud (you need to purchase SD card or DMSS cloud separately).

## 6.4.3 Subscribing Alarms

Subscribe access control alarm messages, so that you can receive the alarm notifications on your mobile device.

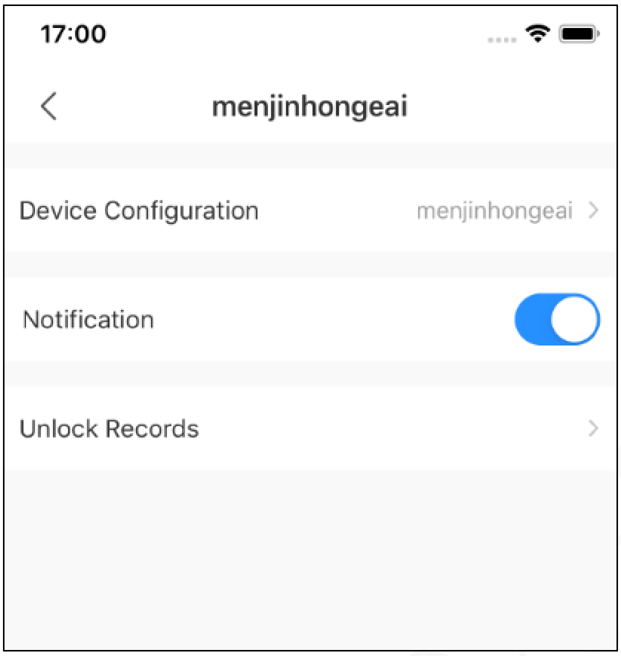
Step 1 Log in to DMSS.

Step 2 Tap Access.

Step 3 Tap , and then find and tap the face recognition terminal you are going to subscribe alarm message for.

Step 4 Tap ○ next to **Notification** to enable automatic push of access control alarms. ● indicates that the notification is enabled.

Figure 6-41 Subscribe alarm message



17:00

menjinhongeai

Device Configuration menjinhongeai

Notification ●

Unlock Records

## 6.4.4 Commissioning

### Preparation

- Face recognition terminal and turnstile are correctly installed and connected.
- Unlock mode, face database and face recognition parameters are correctly configured on the face recognition terminal.
- Face recognition terminal is added to DMSS.
- Video and image storage is configured on DMSS.
- Alarm notification is subscribed on DMSS.

### Objectives

DMSS displays face recognition, temperature measurement and mask detection alarms.

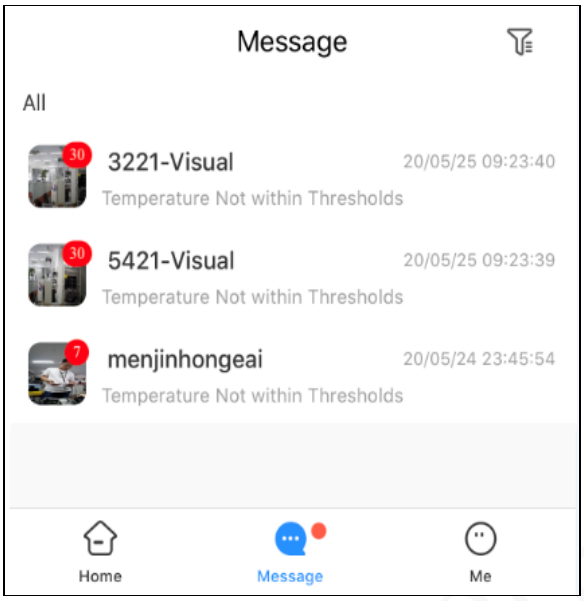
### Procedure

Step 1 Trigger a human body temperature alarm (temperature higher than the threshold).

Step 2 Log in to DMSS.

Step 3 Tap Message , find and tap the name of the face recognition terminal, and then check whether the body temperature alarm is displayed.

Figure 6-42 Alarm notifications grouped by device



Message

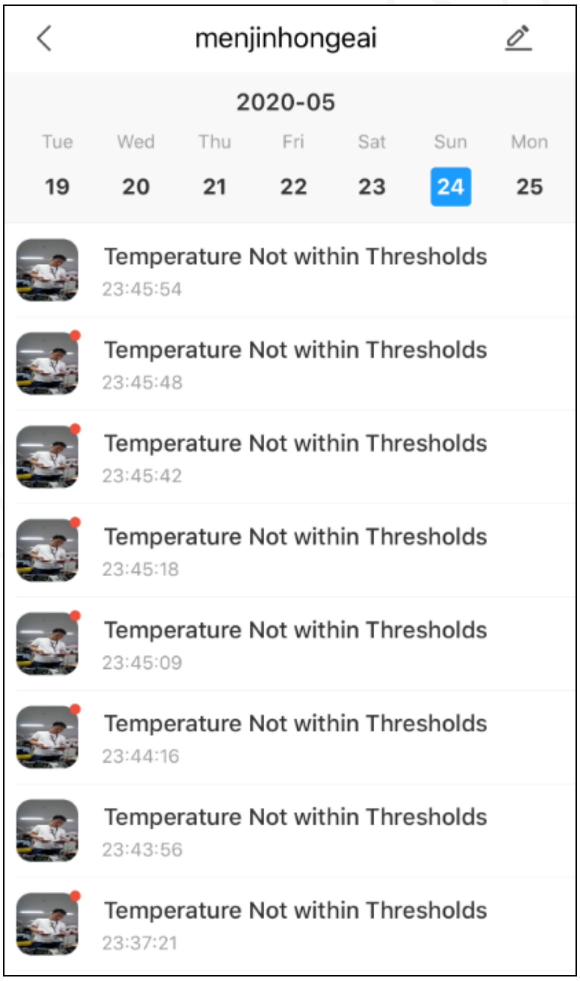
All

3221-Visual 20/05/25 09:23:40
Temperature Not within Thresholds

5421-Visual 20/05/25 09:23:39
Temperature Not within Thresholds

menjinhongeai 20/05/24 23:45:54
Temperature Not within Thresholds

Figure 6-43 Alarm messages



menjinhongeai

2020-05

| Tue | Wed | Thu | Fri | Sat | Sun | Mon |
|---|---|---|---|---|---|---|
| 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Temperature Not within Thresholds
23:45:54

Temperature Not within Thresholds
23:45:48

Temperature Not within Thresholds
23:45:42

Temperature Not within Thresholds
23:45:18

Temperature Not within Thresholds
23:45:09

Temperature Not within Thresholds
23:44:16

Temperature Not within Thresholds
23:43:56

Temperature Not within Thresholds
23:37:21

# 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.

**ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.**

Address: No.1199, Bin'an Road, Binjiang District, Hangzhou, P.R. China