



# Elevator Control Solution




## Deployment Guide



# Foreword

## Safety Instructions

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

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

## Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	May 2021

## 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.

## Interface Declaration

This manual mainly introduces the relevant functions when you use the device. The interfaces used for manufacture, returning to the factory for inspection, and locating fault are not described in this manual. Please contact technical support if you need information about these interfaces.

## About the Guide

- The Guide is for reference only. If there is inconsistency between the Guide and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the Guide.
- The Guide would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper manual, CD-ROM, QR code or our official website. If there is inconsistency between paper manual and the electronic version, the electronic version shall prevail.

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

# Important Safeguards and Warnings

## Electrical Safety

- All installation and operation should conform to your local electrical safety codes.
- Use power supply that meets ES1 but does not exceed PS2 limits defined in IEC 62368-1. For specific power supply requirements, refer to device labels.
- 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

<b>Foreword</b> .....	<b>I</b>
<b>Important Safeguards and Warnings</b> .....	<b>III</b>
<b>1 Overview</b> .....	<b>1</b>
<b>2 Network Diagram</b> .....	<b>2</b>
<b>3 Deployment Process</b> .....	<b>3</b>
<b>4 Installation</b> .....	<b>6</b>
4.1 Cable Connection .....	6
4.1.1 Overview.....	6
4.1.2 DIP Switch.....	7
4.1.3 Connecting Elevator Call Module.....	10
4.1.4 Connecting Elevator Control Module .....	11
4.1.5 Installing Elevator Call/Control Module .....	12
4.2 Installing DSS Pro .....	13
4.2.1 Installing DSS Pro Service .....	13
4.2.2 Logging in to Web Manager .....	17
4.2.3 Licensing DSS Pro .....	17
4.2.4 Installing DSS Pro Control Client.....	20
4.2.5 Logging in to DSS Pro Client.....	23
4.2.6 Licensing .....	25
<b>5 Configuration and Commissioning</b> .....	<b>29</b>
5.1 Configuring Elevator Control/Call Module.....	29
5.1.1 Initializing Elevator Control/Call Module.....	29
5.1.2 Upgrading Elevator Control/Call module.....	29
5.1.3 Configuring Elevator Control/Call Module.....	30
5.2 Configuring Elevator Controller.....	31
5.2.1 Initializing Elevator Controller .....	31
5.2.2 Adding Elevator Control/Call Module to Elevator Controller .....	32
5.3 Configuring VTO and VTH.....	33
5.3.1 Initializing VTO and VTH in Batches .....	33
5.3.2 Configuring VTO and VTH in Batches .....	35
5.3.3 Enabling Elevator Control on VTO .....	36
5.4 Configuring DSS Pro .....	37
5.4.1 Configuring Storage Disk.....	37
5.4.2 Adding Devices .....	39
5.4.3 Configuring Video Recording Plan .....	43
5.4.4 Binding Video Channel to Elevator Controller .....	43
5.4.5 Configuring Access Permissions.....	44
5.4.6 Configuring Elevator Control Event .....	52
5.5 Commissioning .....	53
5.5.1 Calling Elevator from VTH.....	53
5.5.2 Opening Unit Door from VTH.....	53
5.5.3 Calling Elevator from VTO.....	53

---

**Appendix 1 Cybersecurity Recommendations ..... 54**

# 1 Overview

The elevator control solution is designed for on-line management of elevators. It supports elevator authorization. The elevator availability can be controlled by time and people, to make full use of resources. The system has a variety of application modes, supporting card swiping, fingerprint identification and face recognition. The DSS platform supports the classification of elevator usage records, which can be used for analysis as needed.

- Elevator control: Online management, supporting configuring elevator number, name, number of floors, start and end floors, and floor control.
- Elevator control authorization: By department and people. A department is pre-configured with permissions, and people in the department are authorized accordingly. If the department permission is changed, permissions of people in this department changes too.
- Elevator control plan: The solution supports configuring 4 periods of elevator control, which is flexible to use.
- Elevator control method: Diversified application modes, supporting card swiping, fingerprint identification and face recognition.
- Record search: The DSS platform displays card wiping and face recognition records, including number, time, person name, card number, department, elevator name, card type and more.

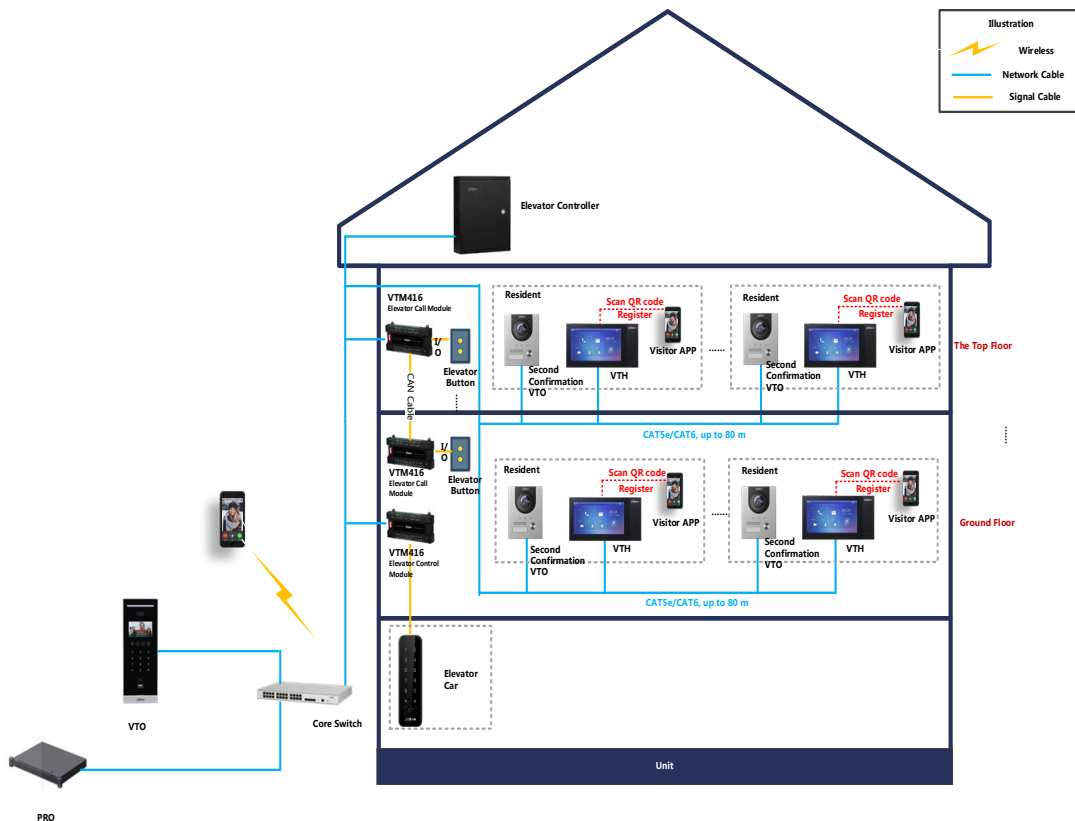


The deployment guide is for reference only. If there is any difference between the guide and the product, the actual product shall prevail.



## 2 Network Diagram

This diagram gives you a quick understanding of networking for this solution. The typical network diagram is shown in the following figure.

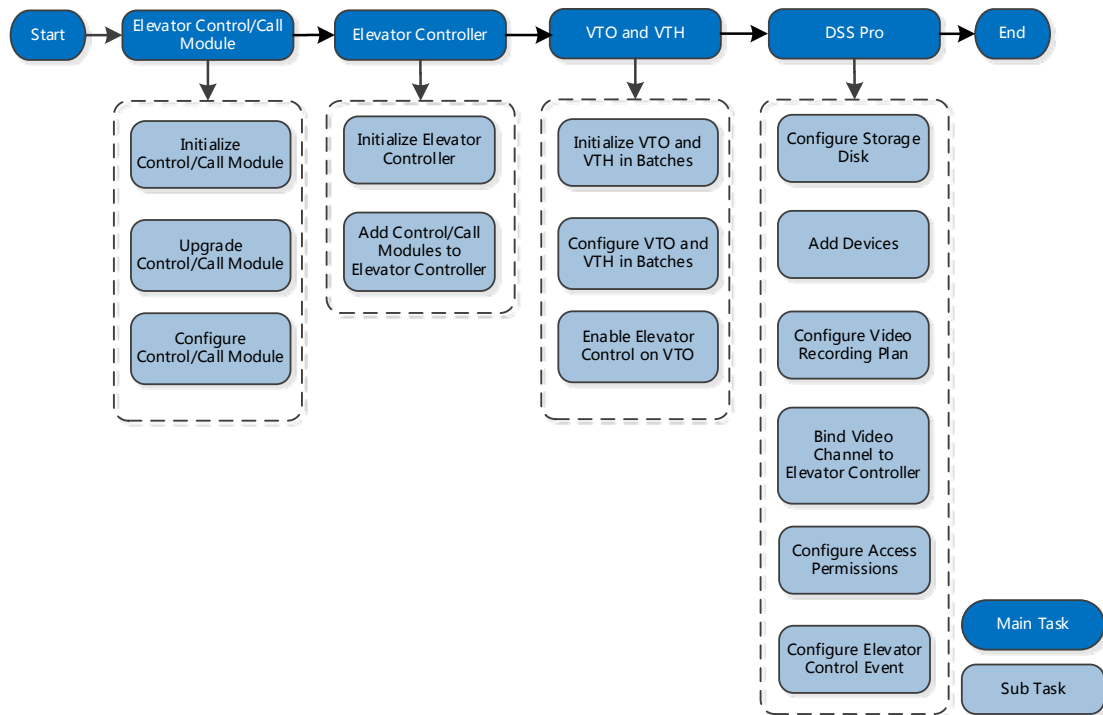


- Elevator controller: Manages elevator control/call modules, the general controller of elevator.
- Elevator control module: Can control up to 16 floors; for more floors, you need to deploy more elevator control modules.
- Elevator call module: Controls the command of calling elevator from home or from the building door.
- Unit VTO (Door Station): Installed at the entrance of the building, for example, the door of the ground floor; Call the homes for opening door.
- Second Confirmation VTO: Installed at the home door; when arriving at the door of the home, a visitor should press the VTO button so that the resident can confirm the visitor
- VTH (Indoor Monitor): Installed in the home for communicating with a visitor, remotely opening door, and calling elevator.
- DSS Pro: Centrally manages the whole system; provides system configurations, such as permissions and rules, and administration operations, such as viewing videos, remotely opening the door and checking records.
- DSS Smart VDP: Installed on mobile phone, working with DSS Pro, and then you can make visitor appointment, create pass, receive push notification, and view visitor records.

### 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.

Figure 3-1 Deployment



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

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

Figure 3-2 SN number



Figure 3-3 Record SN numbers

	A	B	C	D	E
	No.	Device Name	SN	Installation Position	Note
1	1	Star Light Camera	4J04704YAGF0193		
2	2	TPC	5N757U4HAGF0196		
3	3	FR Camera	8H05774YNF019I		
4	4	Audio/Video Camera	3L05704YAKF0684		
5	5	NVR	9R05704YTGf0753		
6	.....				
7					
8					
9					

**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 3-4 Match installation position

	A	B	C	D	E
	No.	Device Name	SN	Installation Position	Note
1	1	Star Light Camera	4J04704YAGF0193	Entrance	
2	2	TPC	5N757U4HAGF0196	Warehouse	
3	3	FR Camera	8H05774YNF019I	Front Door	
4	4	Audio/Video Camera	3L05704YAKF0684	conciierge	
5	5	NVR	9R05704YTGf0753	CCTV Center	
6	.....				
7					

**Step 4** Mark the installation positions on the corresponding packing boxes as planned, and then install them to proper locations. See Figure 3-5 and "4 Installation."

Figure 3-5 Mark installation position



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

Figure 3-6 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	9R05704YTF0753	CCTV Center	192.168.1.14
7	.....				

**Step 6** Configure devices. See "5 Configuration and Commissioning."



- Elevator control module connects to the elevator buttons and reader. One elevator control module supports 16 floors. If there are more than 16 floors, you need to add more elevator control modules.
- Elevator call module supports 16 floors, connects to the elevator up and down button. Generally, If there are 16 floors, the elevator call module is installed in the 8<sup>th</sup> floor. If there are more than 16 floors, you need to add more elevator control modules.

## 4.1.2 DIP Switch

To identify the elevator call/control module in the network, you need to dial the DIP switch to set a RS-485 address for it.

Figure 4-2 DIP switch

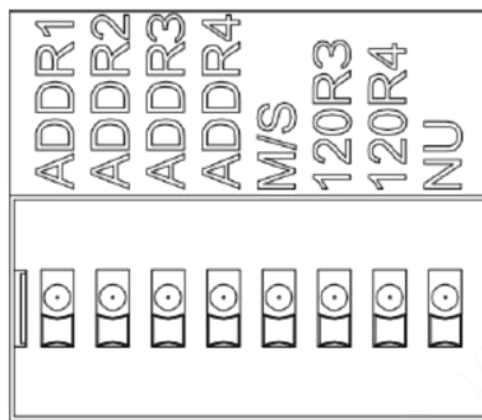


Table 4-1 DIP switch description

Icon	Description
ADDR1-ADDR4	Distinguishes between elevator control and elevator call. ADDR1-ADDR3: . ADDR4:  for elevator control, and  for elevator call. For example, if the current device is for elevator control, dial ADDR4 as .
M/S	Distinguishes between main and sub devices. for main devices, and  for sub devices.

Dial the DIP switch as needed.

Figure 4-3 DIP switch (elevator control module-main)

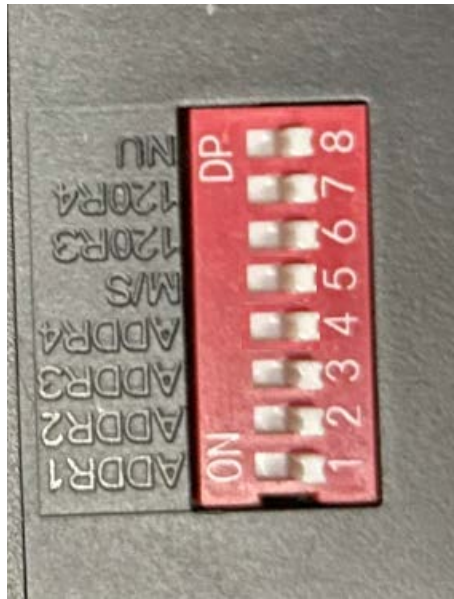


Figure 4-4 DIP switch (elevator control module-sub)

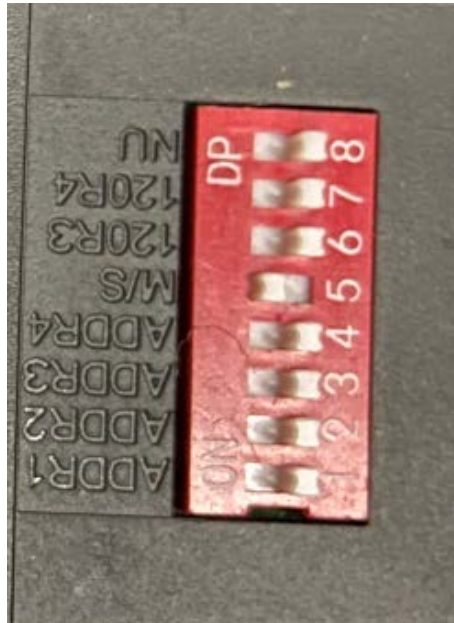


Figure 4-5 DIP switch (elevator call module-main)

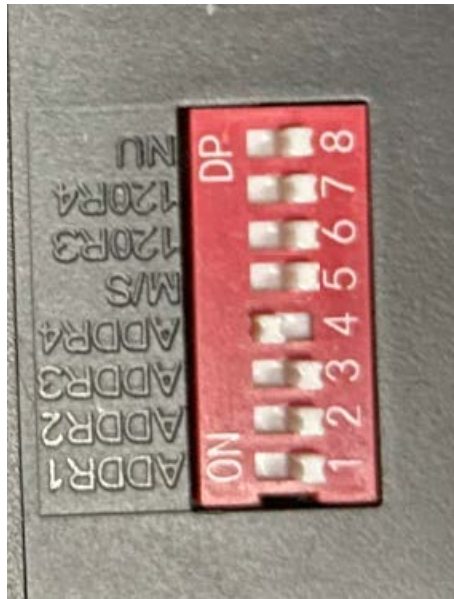
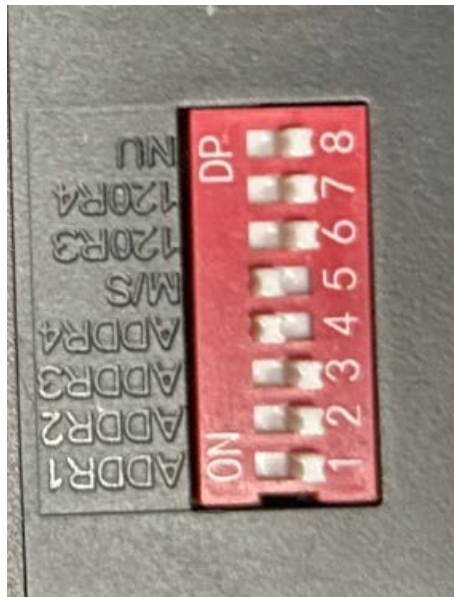


Figure 4-6 DIP switch (elevator call module-sub)





### 4.1.3 Connecting Elevator Call Module

Figure 4-7 Connect elevator call module and elevator up and down button (1)

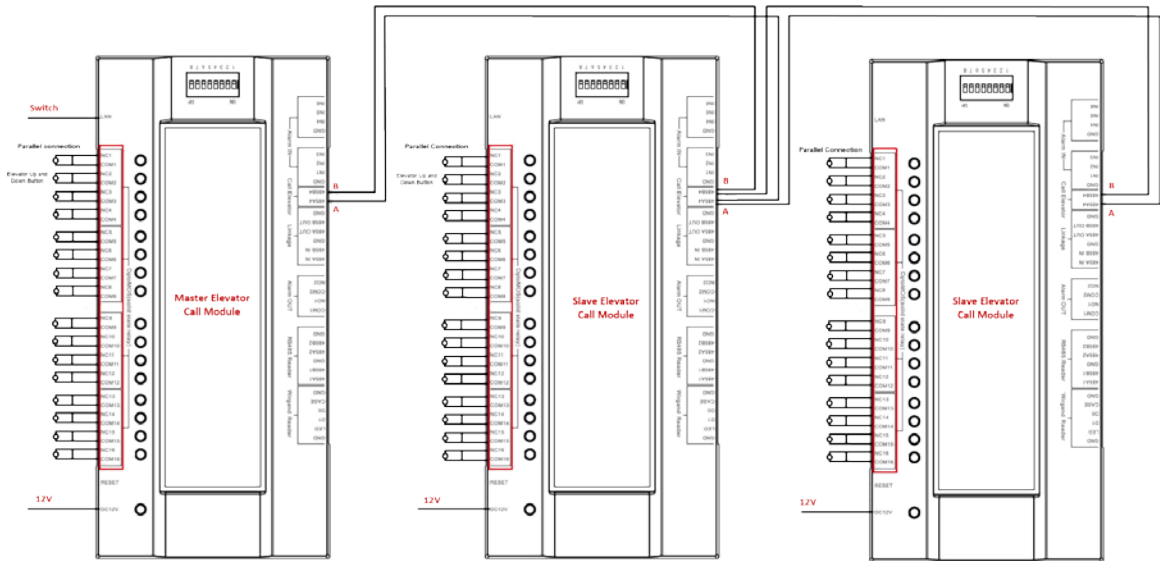
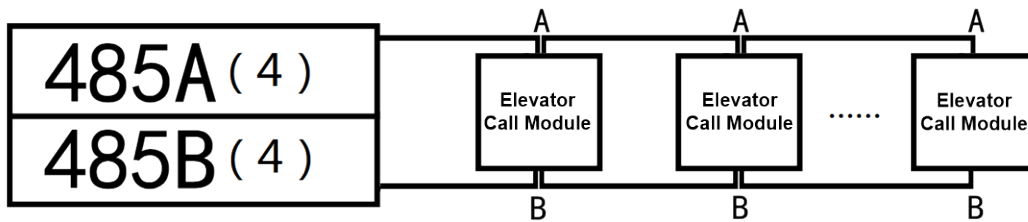
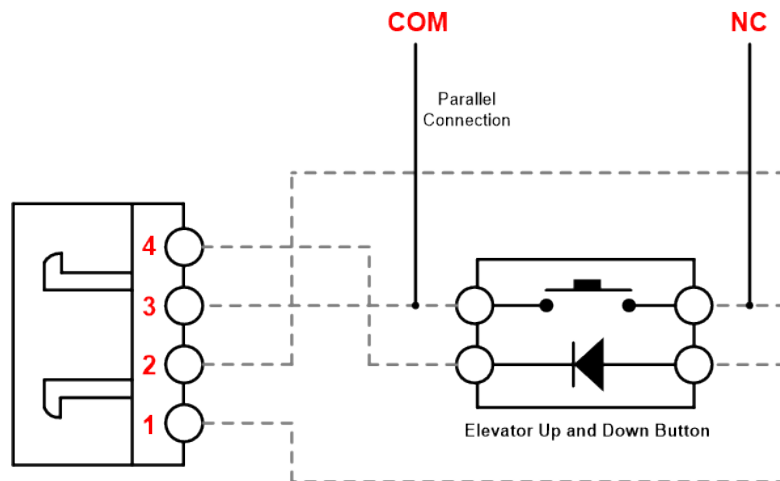


Figure 4-8 Elevator call module cascading



- When there are multiple elevator call modules, cascade the modules through the A port and B port.
- The main elevator call module connects to the switch through LAN port; the sub elevator call modules need not connect to the switch.
- Connect the elevator call module and the elevator up and down buttons through parallel connection.

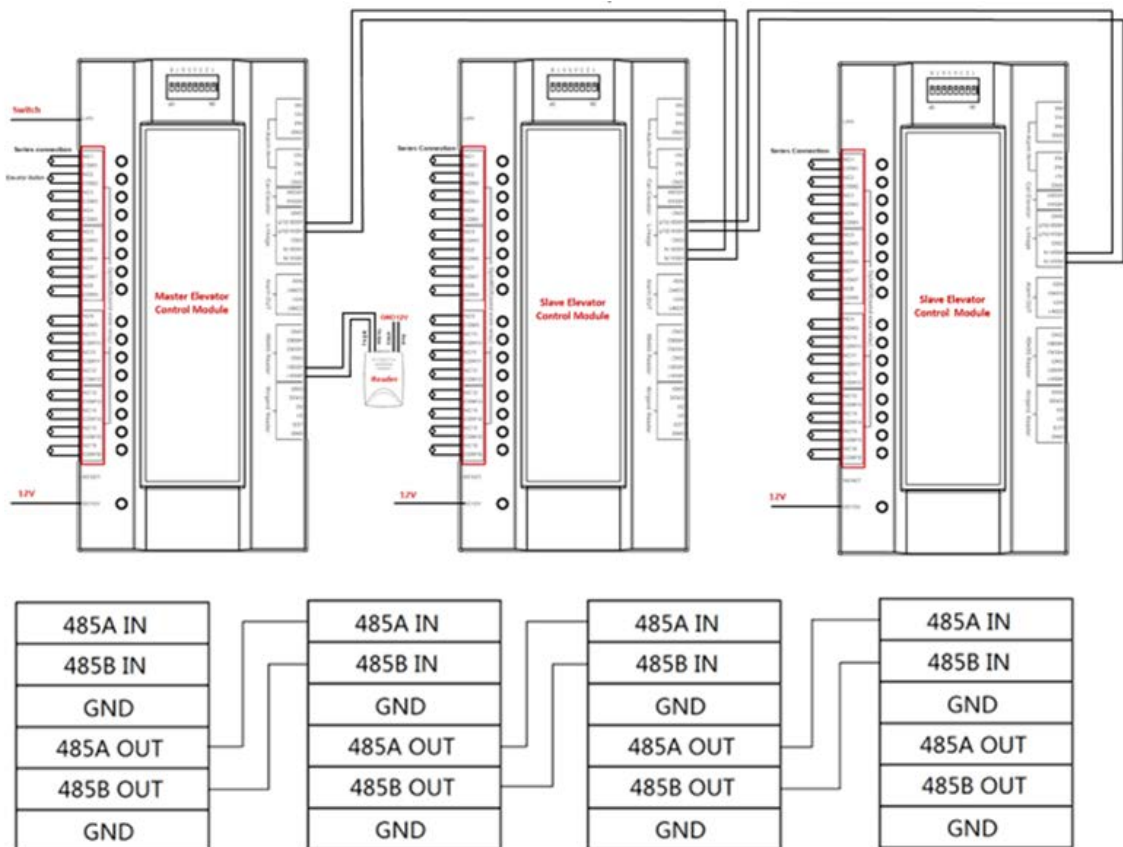
Figure 4-9 Connect elevator call module and elevator up and down button (2)



Generally, for the ground floor, the NC and COM ports of the relay output of the elevator call module are connected in parallel with the elevator up button; for the other floors, the NC and COM ports of the relay output of the elevator call module are connected in parallel with the elevator down button.

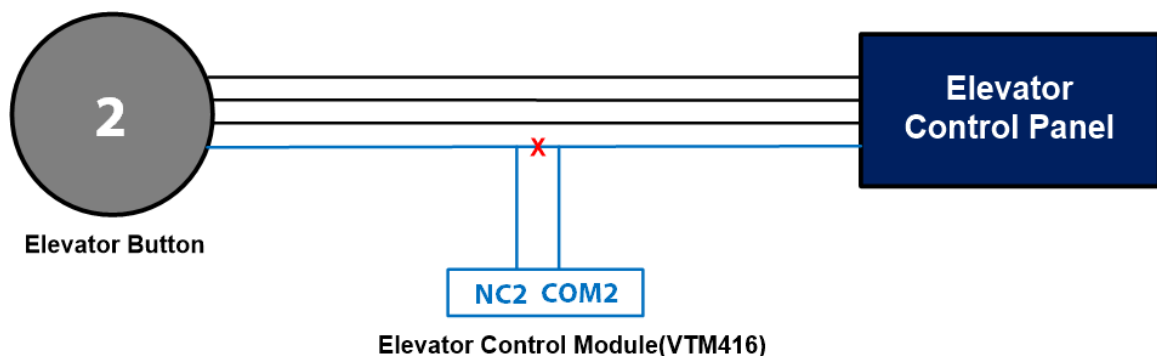
### 4.1.4 Connecting Elevator Control Module

Figure 4-10 Connect elevator control module, elevator button and reader



- If there are multiple elevator control modules, they need to be cascaded. Up to 7 modules can be cascaded.
- The main elevator call module connects to the switch through LAN port; the sub elevator call modules need not connect to the switch.
- Elevator control module connects in series with elevator button.
- Elevator control module does not provide power supply for readers. The reader needs separate DC 12V power supply.

Figure 4-11 Connect elevator control module and elevator button



- The relay output port of the elevator control module is connected in series with the elevator button.
- Button 1 connects to NC1, COM1; button 2 connects to NC2, COM2.
- One elevator control module supports 16 floors. If there are more than 16 floors, you need to add elevator control modules.



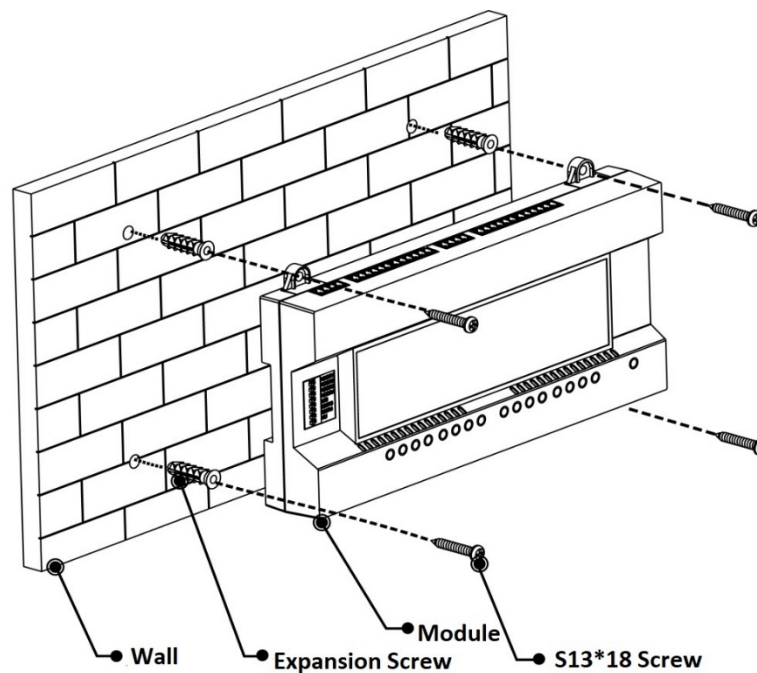
When you set Port Mode to Free Access for a floor during configuring elevator control module, do not connect the elevator control module and the elevator button of the floor through signal cable. For example, you set Port Mode to Free Access for Floor 1, do not connect button 1 to NC1, COM1 on the elevator control module. For details of elevator control module configuration, see "5.1.3 Configuring Elevator Control/Call Module"

## 4.1.5 Installing Elevator Call/Control Module

The installation method of elevator call module and elevator control module is the same.

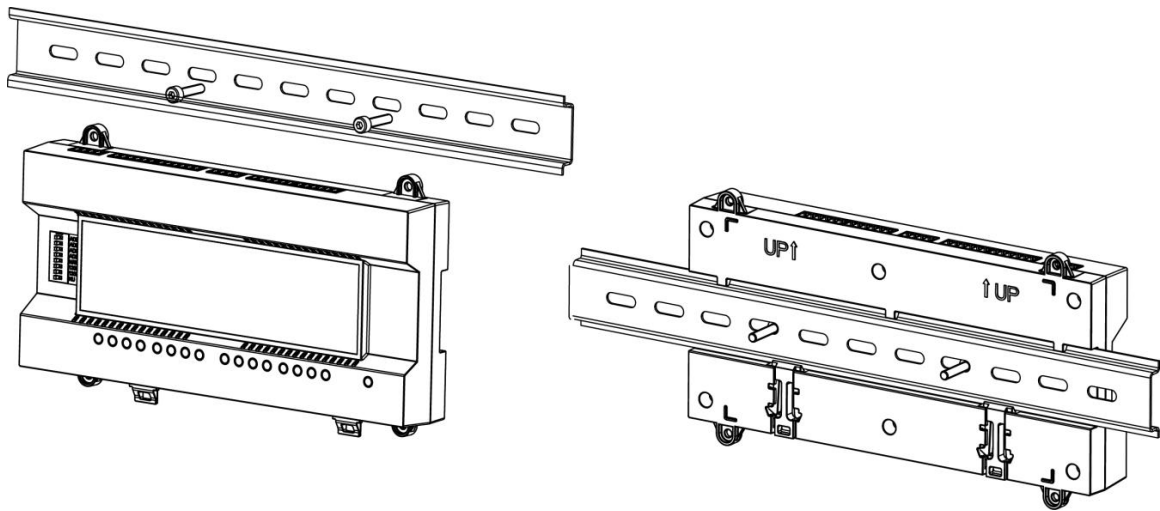
- Install elevator call/control module on the wall

Figure 4-12 Install elevator call/control module on the wall



- Install elevator call/control module on the guide rail

Figure 4-13 Install elevator call/control module on the guide rail



- Step 1** Fix the U-shaped guide rail onto the wall with screws.
- Step 2** Buckle the upper rear part of the device into upper groove of the U-shaped guide rail.
- Step 3** Push the snap joint at the bottom of the device upwards. The installation is completed when you hear the fitting sound.

## 4.2 Installing DSS Pro



DSS Pro is the central platform that manages the whole system and provides video and alarm monitoring. You need to install the DSS service on the server and the Control Client on your PC.

### 4.2.1 Installing DSS Pro Service

Table 4-2 Hardware requirement

Parameter	Hardware Requirement	Operating System
Recommended configuration	<ul style="list-style-type: none"> <li>● CPU: Intel Xeon Silver 4114@ 2.2GHz 10 Core Processor</li> <li>● RAM: 16 GB</li> <li>● Network card: 4 Ethernet port @ 1000 Mbps</li> <li>● Hard drive type: HDD 1TB</li> <li>● DSS installation directory space: Over 500 GB</li> </ul>	<ul style="list-style-type: none"> <li>● Win10-64bit</li> <li>● Windows server 2008</li> <li>● Windows server 2012</li> <li>● Windows server 2016</li> <li>● Windows server 2019</li> </ul>

<p>Minimum configuration</p>	<ul style="list-style-type: none"> <li>• CPU: E3-1220 v5@2.60GHz 4 Core Processor</li> <li>• RAM: 8 GB</li> <li>• Network card: 2 Ethernet port @ 1000 Mbps</li> <li>• Hard drive type: HDD 1TB</li> <li>• DSS installation directory space: Over 500 GB</li> </ul>	<p>Win10-64bit</p>
------------------------------	---	--------------------

Step 1 Double-click  .  


Program name includes version number and program data. Confirm it before installation.

Figure 4-14 Agreement interface



Step 2 Click **agreement**, read the agreement, and then select the **I have read and agree to the DSS agreement** check box. Click **Next**.

Step 3 Select **Main** for server type, and then click **Next**.

Figure 4-15 Select installation path



**Step 4** Select the installation path. You can click **Browse** to customize the installation directory. After selecting installation directory, the system displays the required space and current free space.



- It is not recommended that you install the platform into Disk C because features such as face recognition require higher disk performance.
- If the **Install** button is gray, check whether the installation directory is correct, or if free space is larger than the required space.

**Step 5** Click **Install**.

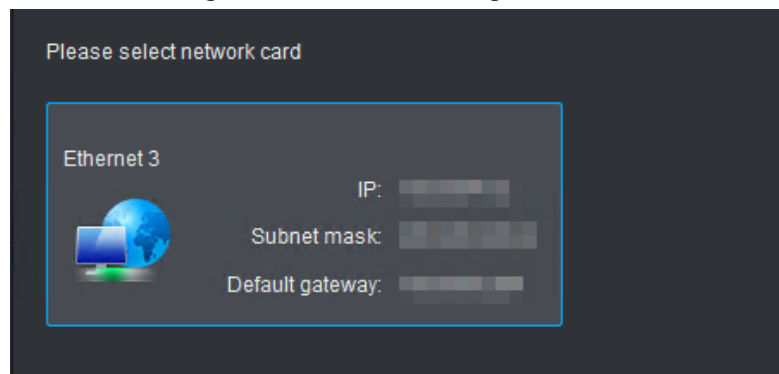
The installation process takes about 3 to 5 minutes. The **Run** interface is displayed after the installation is completed.

Figure 4-16 End of installation



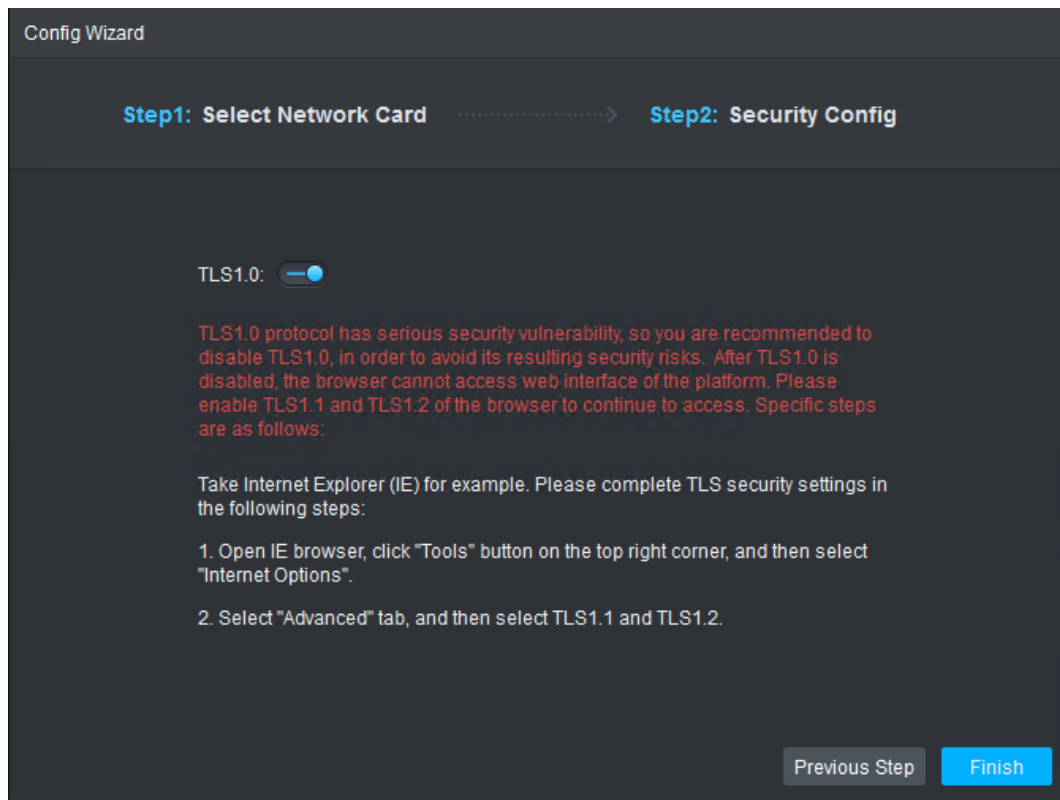
Step 6 Click **Run**.

Figure 4-17 Network config



Step 7 Select a network card, and then click **OK**.  
The security setting interface is displayed.

Figure 4-18 Enable TLS1.0



Step 8 Enable or disable TLS1.0 protocol as screen instructions.

Step 9 Click **OK**.

## 4.2.2 Logging in to Web Manager

On the Web Manager, you can activate the platform, and then system and business configurations.

Step 1 Enter platform IP address in the browser, and then press Enter.

Step 2 Enter username and password, and then click **Login**.



- You are required to modify the password when logging in for the first time.
- Please add the platform IP address into the trusted sites of browser if it is your first time to log in.

## 4.2.3 Licensing DSS Pro

Activate the platform with a paid license the first time you log in to it.



For how to buy a license, contact the sales personnel.

Step 1 On the **Home** interface of the Web Manager, click **Activate License**.

Step 2 Select an activation method.

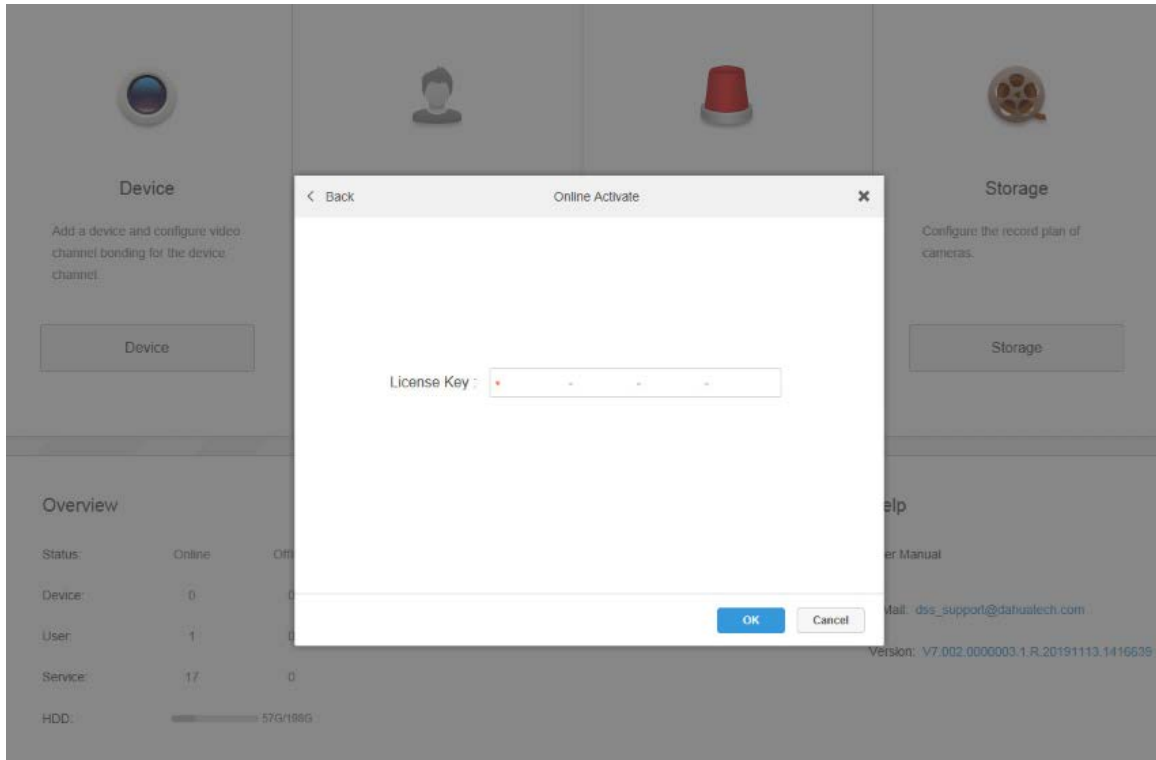
- Online activation

Select **Online Activate** if the platform server is connected to the Internet.



- Offline activation
  - Select **Offline Activate** if the platform server has no Internet access.
- ◇ Online activation
  - 1) On the activation method interface, select **Online Activate**.

Figure 4-19 Online activate

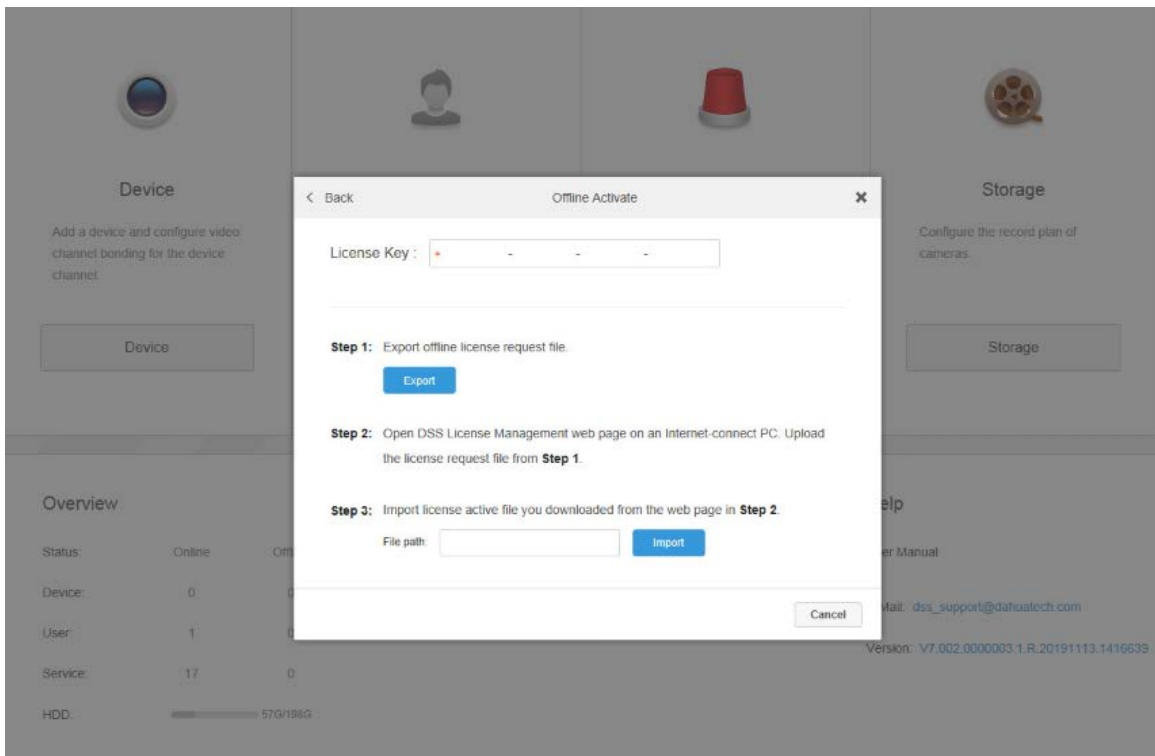


- 2) Enter the new license key, and then click **OK**.

After the license is activated successfully, you can click **Details of License** to view the details of your license capacity.

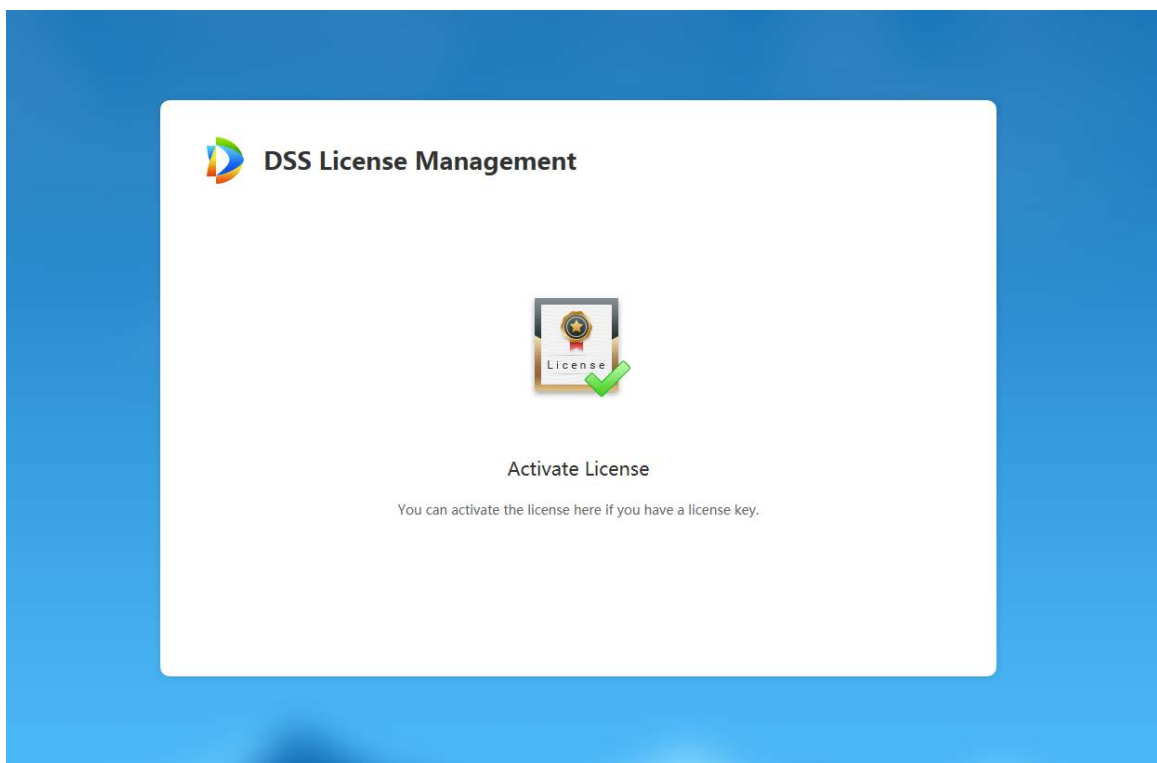
- ◇ Offline activate
  - 1) On the activation method interface, select **Offline Activate**.

Figure 4-20 Offline activate



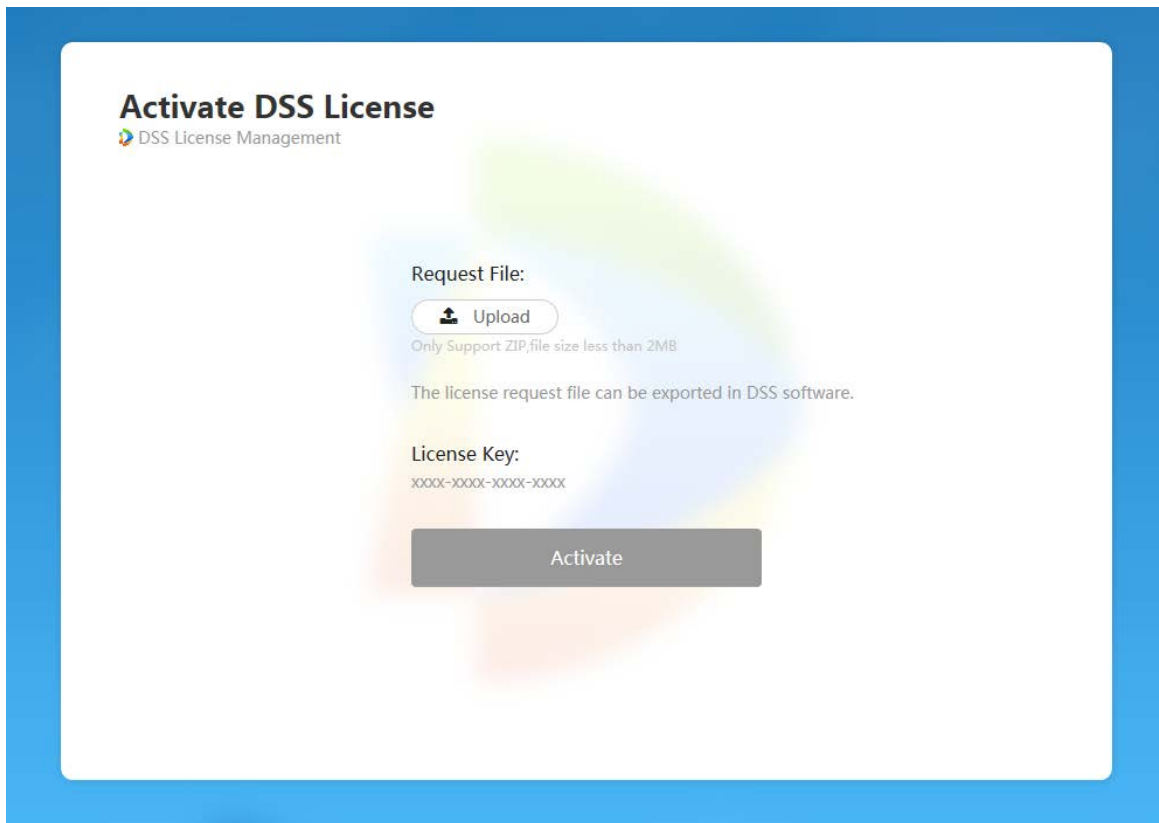
- 2) Enter the license code in the **License Key** box.
- 3) Click **Export** to export the license request file.
- 4) Move the request file to a computer with Internet access. On that computer, open the system email that contains your license, and then click the web page address to go to the license management page.

Figure 4-21 License management web page



- 5) Click **Activate License**.

Figure 4-22 Upload license request file



- 6) Click **Upload**, select the license request file, and then when you are prompted **uploaded successfully**, click **Activate**.

The success interface is displayed, where a download prompt is displayed asking you to save the license activation file.

- 7) On the success interface, click **Save** to save the file, and then move the file to back to the computer where you exported the license request file.
- 8) On the **Offline Activate** interface, click **Import**, and then follow the onscreen instructions to import the license activation file.

After you are prompted that the platform license is activated, you can click **Details of License** to view license capability details.

## 4.2.4 Installing DSS Pro Control Client

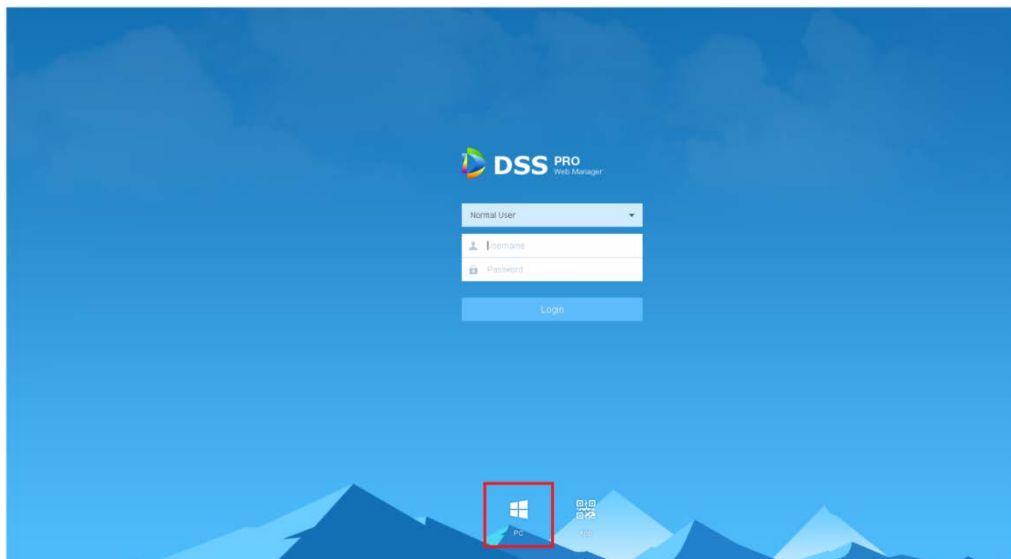
On the Control Client, you can perform daily monitoring.


Table 4-3 Hardware requirements

Parameters	Description
Recommended Configuration	<ul style="list-style-type: none"> <li>• CPU: i5-6500</li> <li>• Main frequency: 3.20 GHz</li> <li>• Memory: 8 GB</li> <li>• Graphics: Inter HD Graphics 530</li> <li>• Network Card: Gigabit Network Card</li> <li>• HDD Type: HDD 1T</li> <li>• DSS client installation space: 200 GB</li> </ul>
Min. Configuration	<ul style="list-style-type: none"> <li>• CPU: i3-2120</li> <li>• Memory: 4 GB</li> <li>• Graphics: Inter(R) Sandbridge Desktop Gra</li> <li>• Network Card: Gigabit Network Card</li> <li>• HDD Type: HDD 300 GB</li> <li>• DSS client installation space: 100 GB</li> </ul>

**Step 1** Enter IP address of DSS Pro into the browser and then press Enter.

Figure 4-23 Log in to the web manager



**Step 2** Click  to download the client.

**Step 3** Double-click the client setup.exe and begin installation.

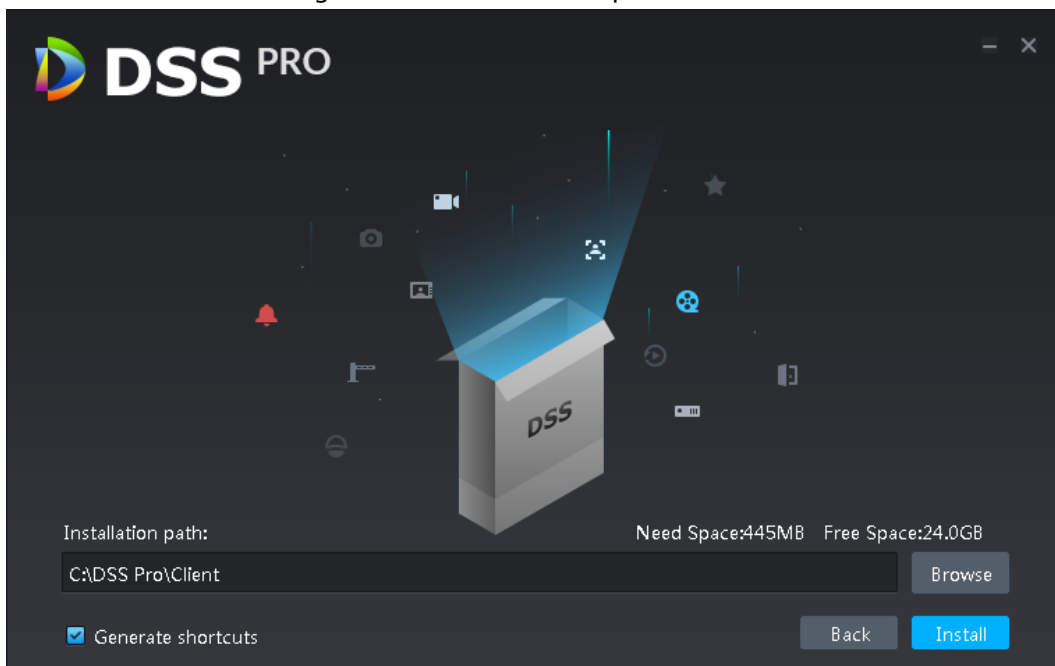
Figure 4-24 Accept agreement



**Step 4** Select a language, select the **I have read and agree DSS agreement** check box and then click **Next**.

**Step 5** Select installation path.

Figure 4-25 Set installation path



**Step 6** Click **Install** to install the client.

System displays installation process. It takes 3 to 5 minutes to complete. Please be patient.

Figure 4-26 Installation completed



Step 7 Click **Run** to run the client.

## 4.2.5 Logging in to DSS Pro Client

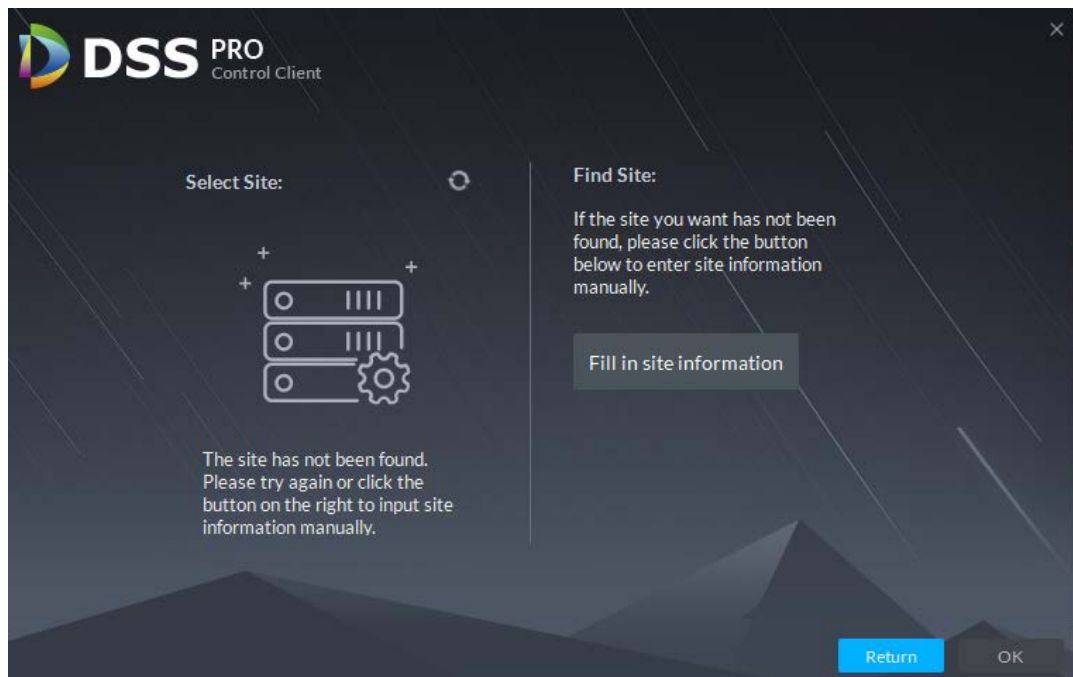
Step 1 Double-click  on the desktop.

- The first time you log in, the following interface is displayed, which proceeds to Step 1.



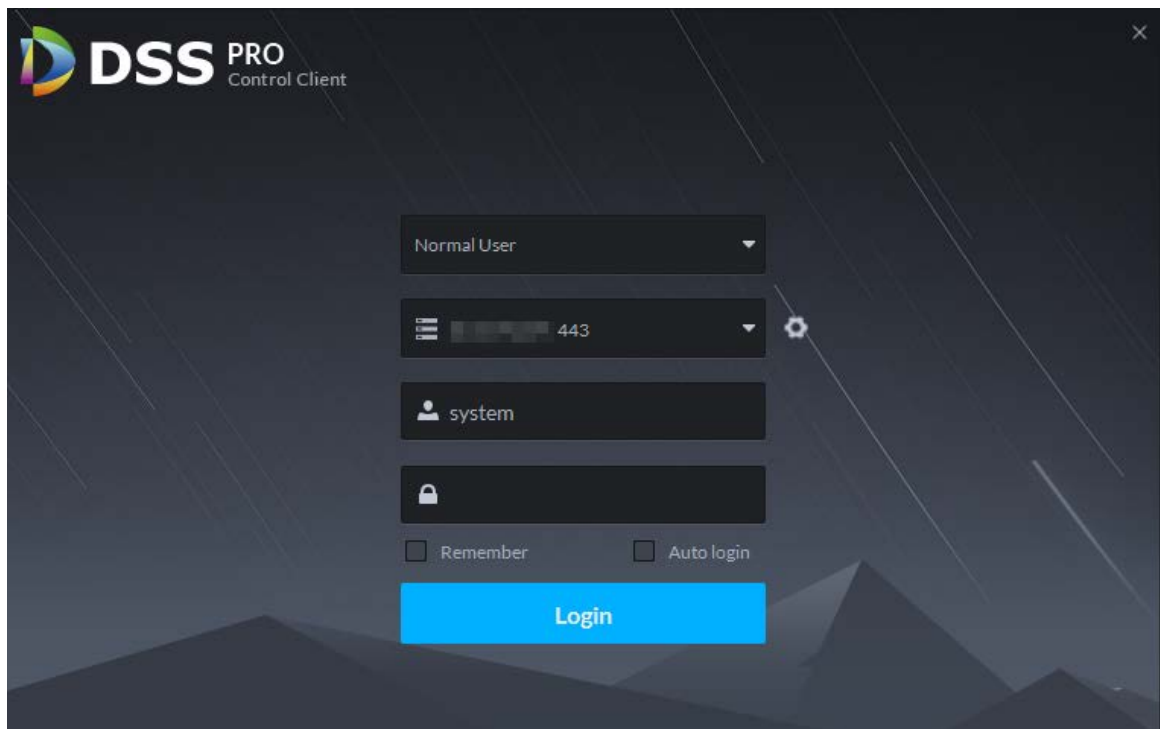
If you have not logged in to Web Manager to initialize the platform, you are required to select a DSS site, set system username and password, and set password protection questions. The questions are used for resetting password in the future when needed.

Figure 4-27 First-time login



- For second-time login or future login, the following interface is displayed, which proceeds to Step 2.

Figure 4-28 Log in to the control client



- Step 1 Select the detected server on the left of the interface, or click **Fill in site** information, enter IP address and port number, and then click **OK**.
- Step 2 Enter **Username**, **Password**, **Server IP** and **Port**. Server IP means the IP address to install DSS Pro server or PC. Port is 443 by default.
- Step 3 Click **Login**.

## 4.2.6 Licensing

Activate the platform with a trial or formal license for first-time login. Otherwise you cannot use the platform.

To activate your license, see the following procedures.

**Step 1** Log in to DSS Pro Web Manager.

**Step 2** Click **Activate License**.

Figure 4-29 Update license

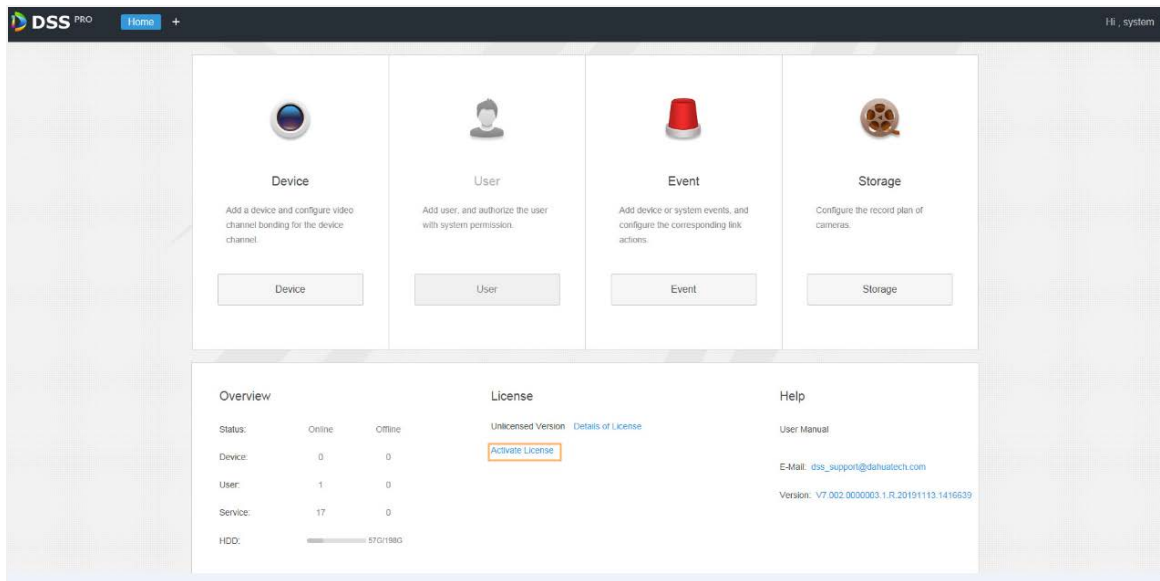
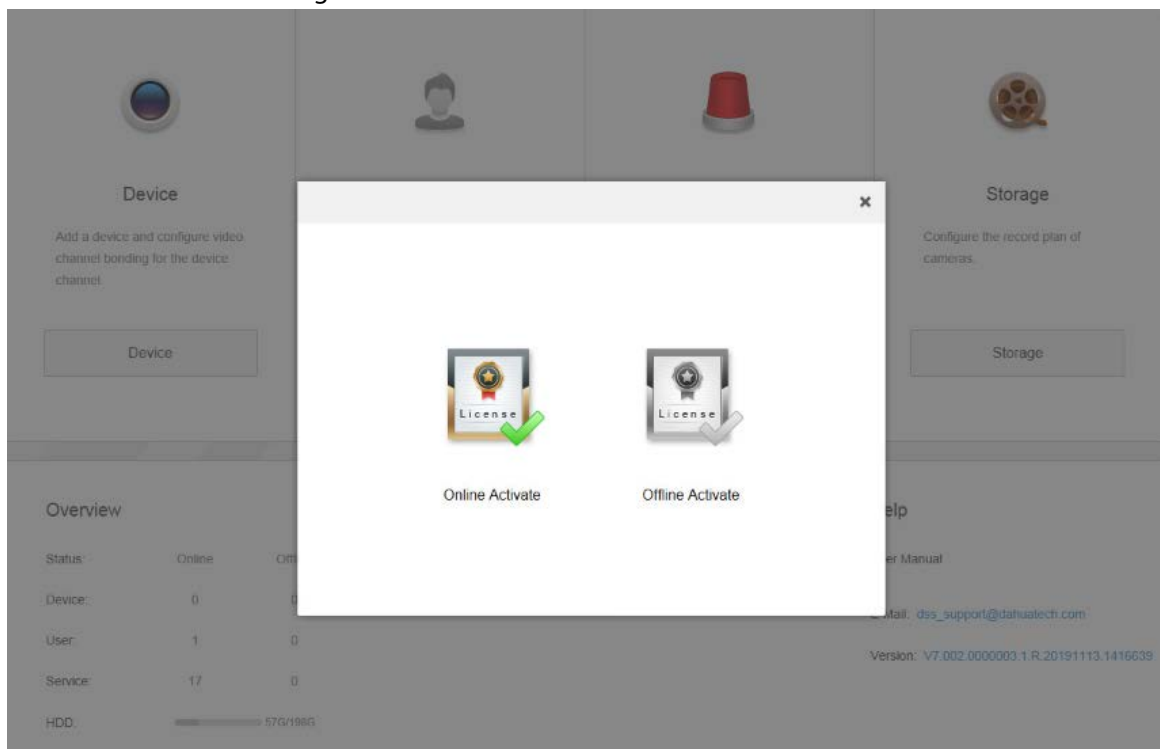


Figure 4-30 Activation method selection



**Step 3** Select an activation method.

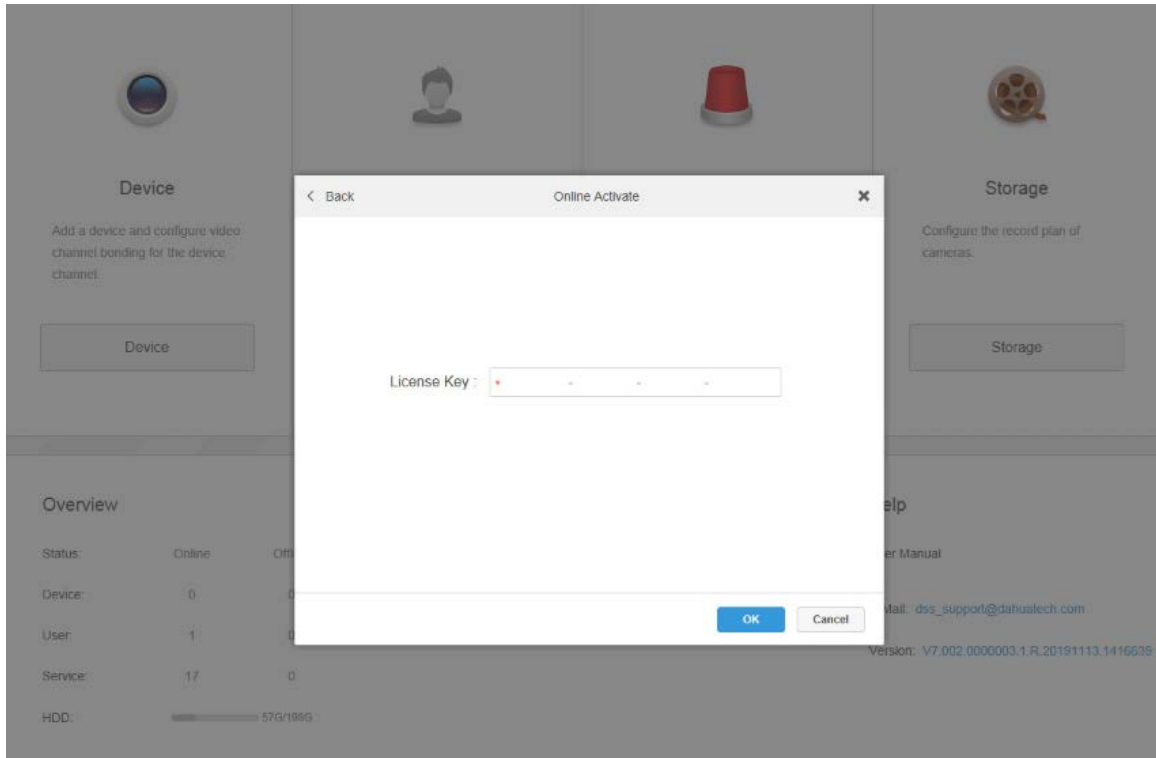
There are two ways to activate the license.

- Online activation  
Select **Online Activate** if the platform server is connected to the Internet.



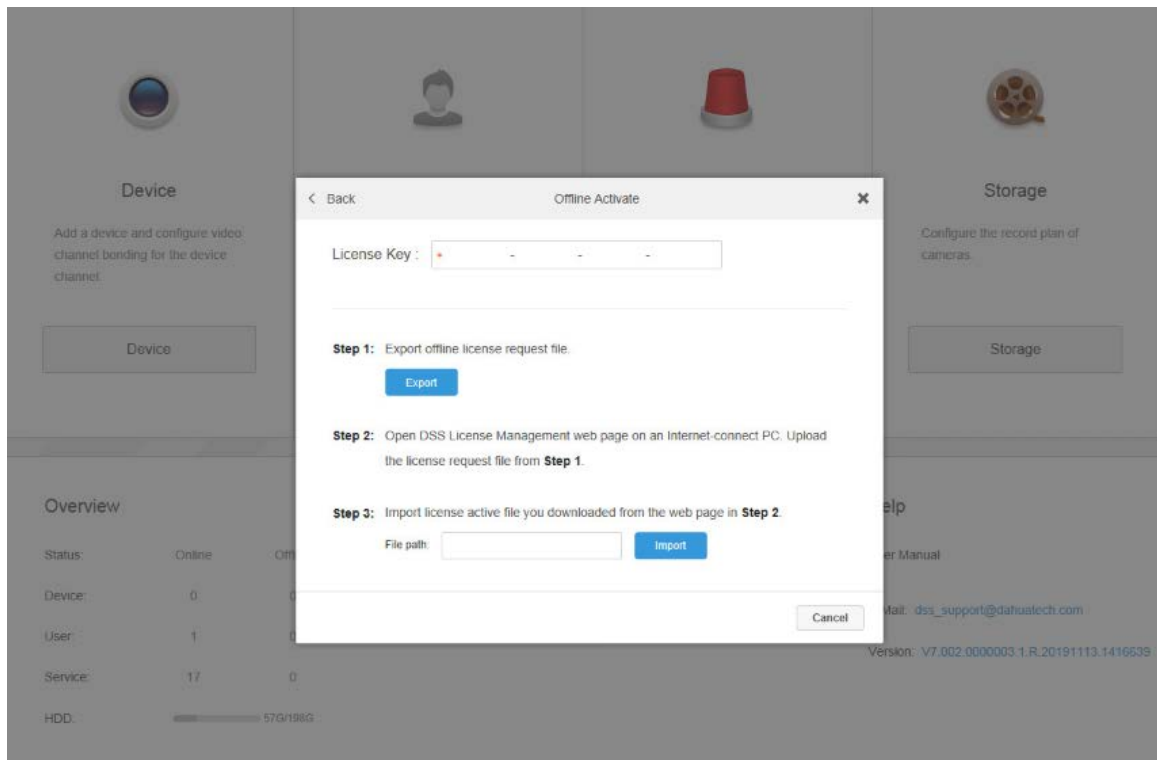
- Offline activation
  - Select **Offline Activate** if the platform server is disconnected from the Internet.
- ◇ Online activation
  - 1) On the activation method interface, select **Online Activate**.

Figure 4-31 Online activate



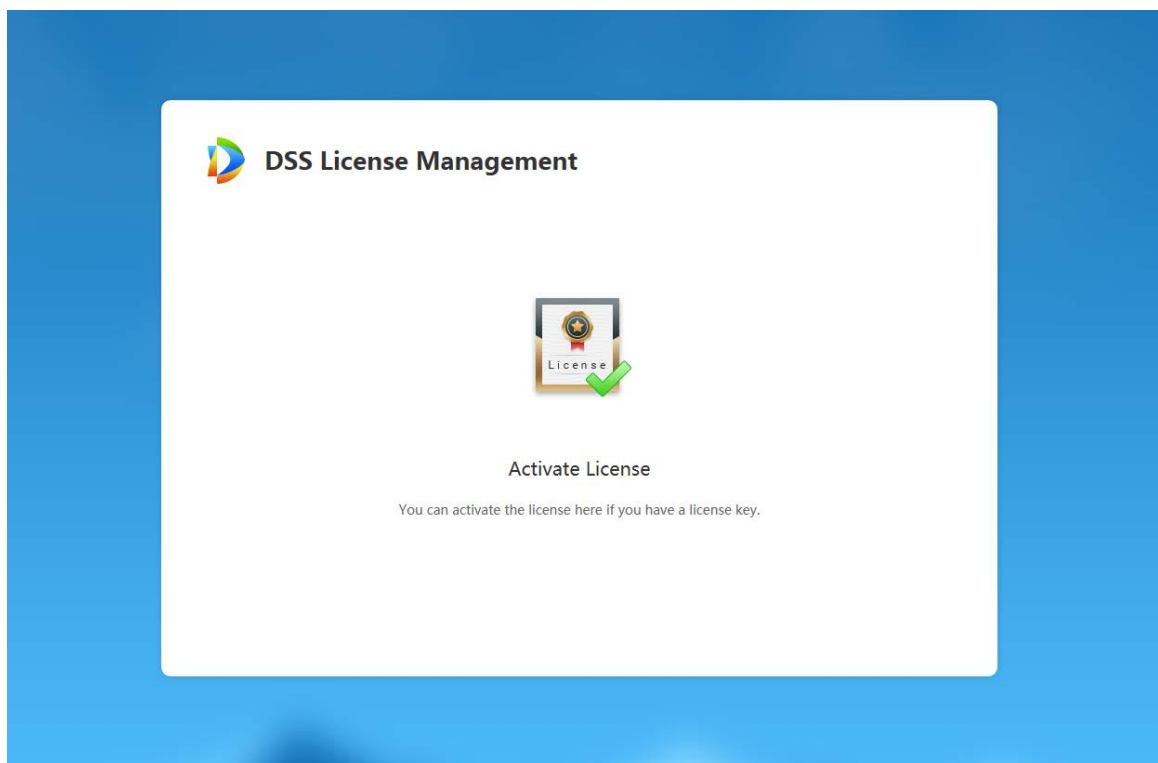
- 2) Enter the new license key, and then click **OK**.
    - After the license is activated successfully, you can click **Details of License** to view the details of your license capacity.
- ◇ Offline activate
    - 1) On the activation method interface, select **Offline Activate**.

Figure 4-32 Offline activate



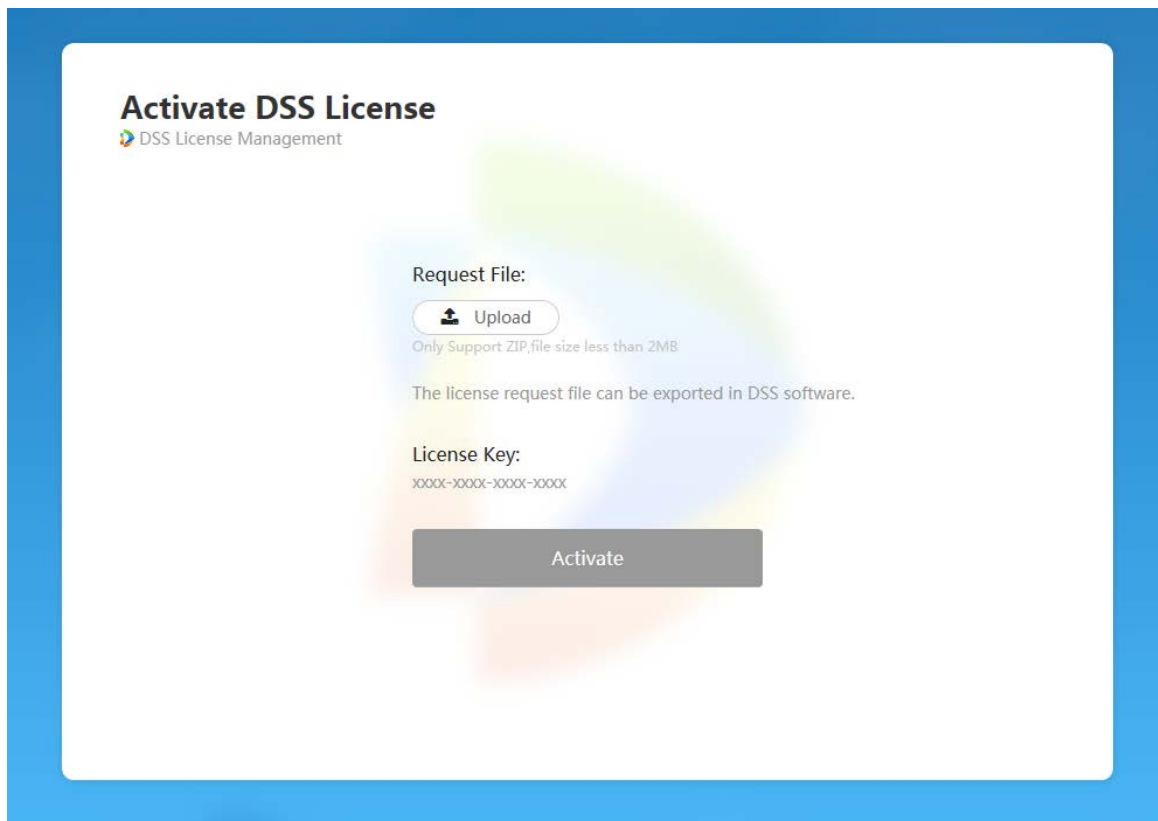
- 2) Enter the license code in the **License Key** box.
- 3) Click **Export** to export the license request file.
- 4) Move the request file to a computer that is connected to the Internet. On that computer, open the system email that contains your license, and then click the web page address to go to the license management page.

Figure 4-33 License management web page



- 5) Click **Activate License**.

Figure 4-34 Upload license request file



- 6) Click **Upload**, select the license request file, and then when you are prompted **uploaded successfully**, click **Activate**.  
The success interface is displayed, where a download prompt is displayed asking you to save the license activation file.
- 7) On the success interface, click **Save** to save the file, and then move the file to back to the computer where you exported the license request file.
- 8) On the **Offline Activate** interface, click **Import**, and then follow the onscreen instructions to import the license activation file.  
After you are prompted that the platform license is activated, you can click **Details of License** to view license capability details.

## 5 Configuration and Commissioning

### 5.1 Configuring Elevator Control/Call Module

#### 5.1.1 Initializing Elevator Control/Call Module

- Step 1 For first-time use, open your browser, enter device IP address in the address bar, and then press Enter.
- Step 2 Follow the on-screen instructions to complete initializing the device.

#### 5.1.2 Upgrading Elevator Control/Call module

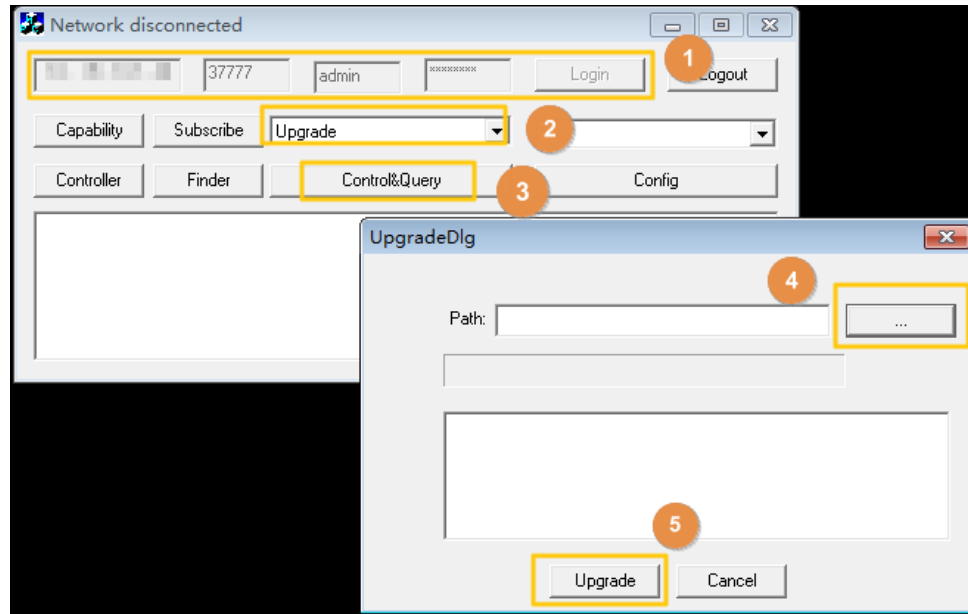
Use AccessControl.exe to upgrade the elevator control/call modules. To acquire the configuration tool, go to Dahua official website, select **Support > Download Center > Software**, and then select the software package according to your operation system. Follow the on-screen instructions to download and install the tool.



Make sure that you have got the software. Otherwise contact your technical support.

- Step 1 Double-click AccessControl.exe., enter the IP address, port (as default), login username and password, and then click **Login**.
- Step 2 Select **Upgrade**, and then click **Control&Query**. See the following figure.
- Step 3 Select the device upgrade files.
- Step 4 Click **Upgrade**.
- Upload Customer\_VTM416\_MCU\_APP\_ENG\_... first, and then repeat step 3-step4 to upload Customer\_WebPacket\_MCU\_APP\_ENG\_... to complete the upgrading.

Figure 5-1 Upgrade



### 5.1.3 Configuring Elevator Control/Call Module

Configure floor parameters on the elevator control module and elevator call module. The floor configuration on the elevator control module and the elevator call module should be consistent.

**Step 1** Log in to elevator control/call module through browser.

**Step 2** Select **Info Link**.

**Step 3** Click **Add**.

**Step 4** Specify parameters.

- Floor NO.: The No. of the floor. For example, 1, the first floor
- Floor Name: The name of the floor. For example, 1
- Lift Ctrl ID: The elevator control/call module DIP number of the floor. For example, 1. This ID is used for identifying the elevator control/call module from the others
- Lift Ctrl Port: The floor number. For example, 1, the 1<sup>st</sup> logical floor on the elevator control/call module
- Port Mode: The access control status of the floor
  - ◇ Lift Access: Under elevator control
  - ◇ Free Access: No control. The floor is always accessible
  - ◇ No Access: The floor is always inaccessible



When you set Port Mode to Free Access for a floor during configuring elevator control module, do not connect the elevator control module and the elevator button of the floor through signal cable. For example, you set Port Mode to Free Access for Floor 1, do not connect button 1 to NC1, COM1 on the elevator control module. For details of elevator control module connection, see "4.1.4 Connecting Elevator Control Module."

Figure 5-2 Configure floor parameters

**Step 5** Click **OK**.

**Step 6** Select **Lift Ctrl Module**, and then click .

**Step 7** Configure the control authorized time of elevator control button.

Figure 5-3 Configure lift ctrl button time

Lift Ctrl ID	Address	Enable	State	L/R Ctrl Button Time(Sec.)	Modify	Delete
1	1	Yes	Online	3		

**Step 8** Click **OK**.

## 5.2 Configuring Elevator Controller

### 5.2.1 Initializing Elevator Controller

**Step 1** For first-time use, open your browser, enter device IP address in the address bar, and then press Enter.

**Step 2** Follow the on-screen instructions to complete initializing the device.

## 5.2.2 Adding Elevator Control/Call Module to Elevator Controller

Add elevator control/call modules. Elevator control module is used for controlling floor access. Elevator call module is used for calling the elevator.

**Step 1** Log in to the elevator controller through browser.

- 1) Enter elevator control/call module IP address in the browser, and then press Enter.
- 2) Enter username and password, and then press Enter.

**Step 2** Select **Lift control module**.

Figure 5-4 Lift control module

	IP Address	Port	Lift control channel	Device Type	Modify
<input type="checkbox"/>	192.168.1.1	37777	1	Lift control module	
<input type="checkbox"/>	192.168.1.2	37777	1	Lift call module	
<input type="checkbox"/>	192.168.1.3	37777	2	Lift control module	
<input type="checkbox"/>	192.168.1.4	37777	2	Lift call module	
<input type="checkbox"/>	192.168.1.5	37777	3	Lift control module	
<input type="checkbox"/>	192.168.1.6	37777	3	Lift call module	
<input type="checkbox"/>	192.168.1.7	37777	4	Lift control module	
<input type="checkbox"/>	192.168.1.8	37777	4	Lift call module	

OK Refresh

**Step 3** To add an elevator control/call module, click

**Step 4** Specify elevator control/call module parameters.

- IP Address: The IP of the elevator control/call module.
- Port: Leave it default.
- Username: Username of the elevator control/call module.
- Password: Password of the elevator control/call module.
- Lift control channel: The channel number of elevator controller. Leave it default.
- Device Type: Select **Lift control module** for elevator control module), and **Lift call module** for elevator call module. Leave it default.

Figure 5-5 Add elevator control/call module

**Modify** ✕

IP Address

Port

Username

Password

Lift control channel  ▼

Device Type  ▼

OK Cancel

**Step 5** Select the check boxes of the elevator control/call modules that you added, and then click **OK**.





Select the **Other Segment Search** check box. Enter the IP address in the **Start IP** box and **End IP** box respectively. Enter the user name in the **Username** box and the password in the **Password** box. The system will search the devices accordingly.



- If you select the **Current Segment Search** check box and the **Other Segment Search** check box together, the system searches devices under both conditions.
- The username and the password are the ones used to log in when you want to modify IP, configure the system, update the device, restart the device, and more.

Step 4 Click **OK**.

Step 5 Select one or several uninitialized devices.

Step 6 Click **Initialize**.

Step 7 Select the devices to be initialized, and then click **Initialize**.



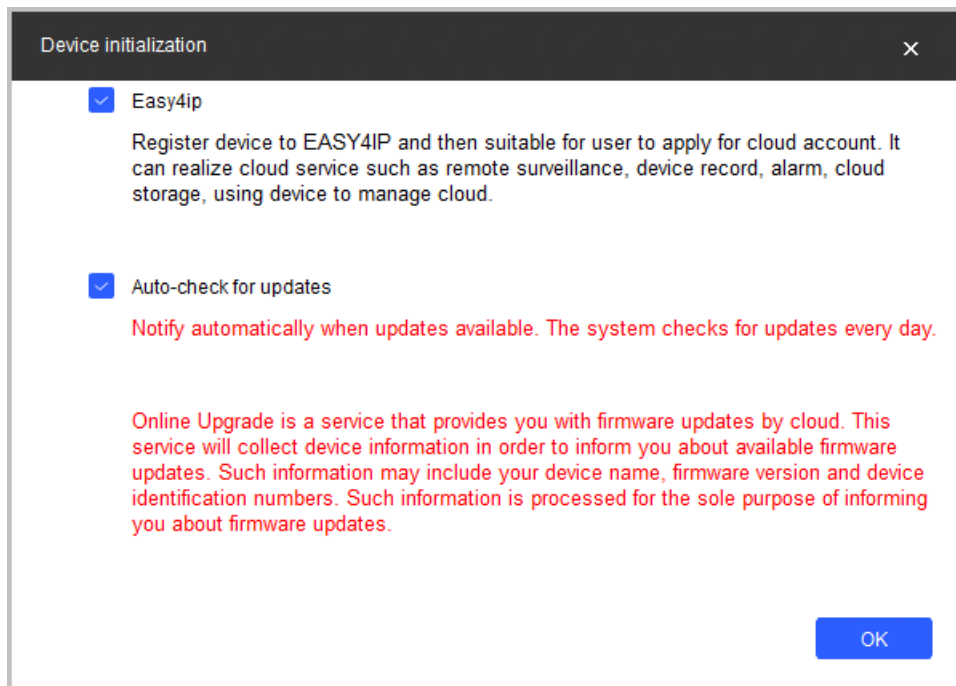
- If you do not provide the reserve information for password reset, you can reset the password only through XML file.
- When initializing multiple devices, the Tool initializes all devices based on the password reset mode of the first selected device.

Figure 5-2 Device initialization (2)

Step 8 Configure the initialization parameters for the device.

Step 9 Click **Next**.

Figure 5-3 Device initialization (3)

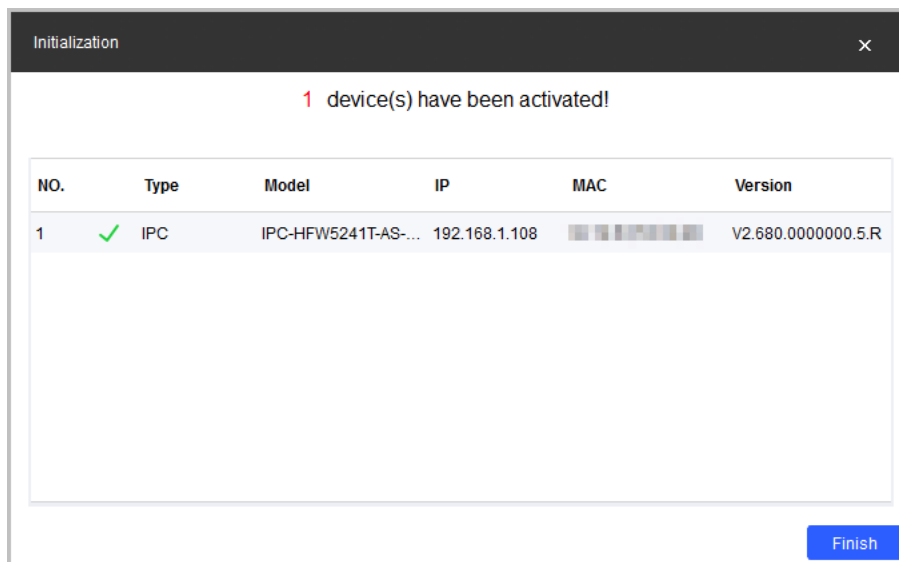


Step 10 Select **Easy4ip** or select **Auto-check for updates** according to the actual needs. If neither, leave them unselected.

Step 11 Click **OK** to initialize the device.


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

Figure 5-4 Initialization



Step 12 Click **Finish**.

### 5.3.2 Configuring VTO and VTH in Batches

Step 1 Run ConfigTool, and then click  **CGI Protocol**.

Step 2 Click **Open Template**, enter IP address, port No., username, password, and CGI commands content, and then save the template and close it.

Figure 5-5 Template

IP Address	Port	Username	Password	CGI Commands Content	protocol (0 - http, 1 - https)	Result
192.168.1.100	8080	admin	admin	/cgi-bin/.../.../...	0	0
192.168.1.100	8080	admin	admin	/cgi-bin/.../.../...	0	0
192.168.1.100	8080	admin	admin	/cgi-bin/.../.../...	1	1

Table 5-1 Parameter description of the template

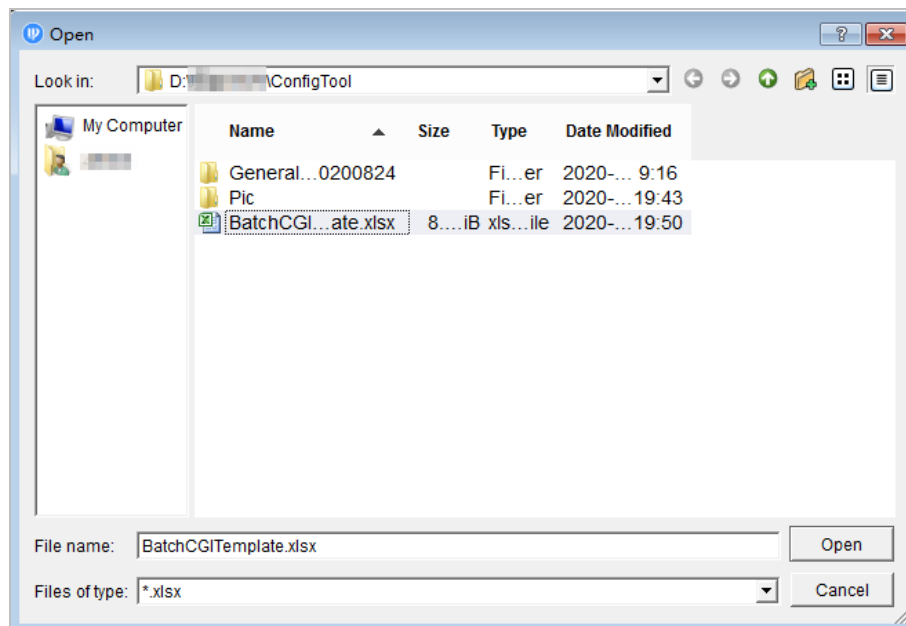
Parameter	Description
IP Address	Enter the device IP, port, login username and password.
Port	
Username	
Password	
CGI Commands Content	The command path of the device CGI configuration. Sending configuration through non-default port is available.
Protocol (0-http, 1-https)	Http and https are available.
Result	The result of the CGI command execution.

**Step 3** Return to CGI protocol interface, and click **Table Config**.

**Step 4** Select the completed template, and click **Open** to import the template. The devices in the template will be configured as the template.

After the configuration is completed, the success notice is displayed. And you can check the result in the template.

Figure 5-6 Select a template



### 5.3.3 Enabling Elevator Control on VTO

**Step 1** Log in to VTO through browser.

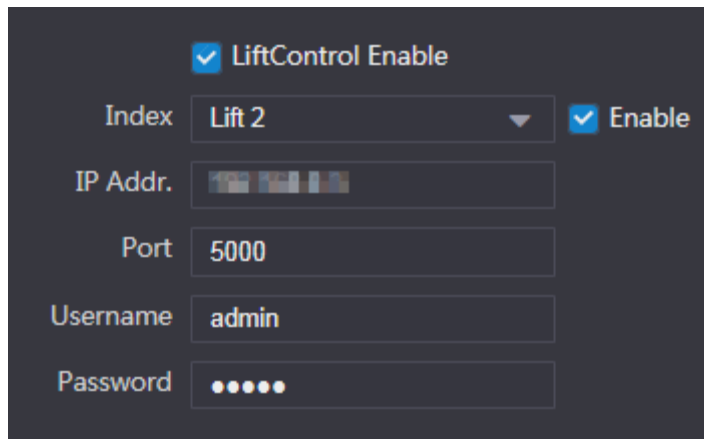
- 1) Enter VTO IP address in the browser, and then press Enter.
- 2) Enter username and password, and then press Enter.

**Step 2** Enable elevator control.

- 1) Select **Local Setting > LiftControl Config**.
- 2) Select the **LiftControl Enable** check box to enable the function.

- ◇ Index: Select an elevator controller ( **Lift 1, Lift 2...**), and then select the **Enable** check box to enable the elevator control module
  - ◇ IP Addr.: The IP address of the selected elevator controller
  - ◇ Port: Leave it default
  - ◇ Username: Username of the elevator controller
  - ◇ Password: Password of the elevator controller
- 3) Click **Save**.

Figure 5-7 Enable elevator control on VTO

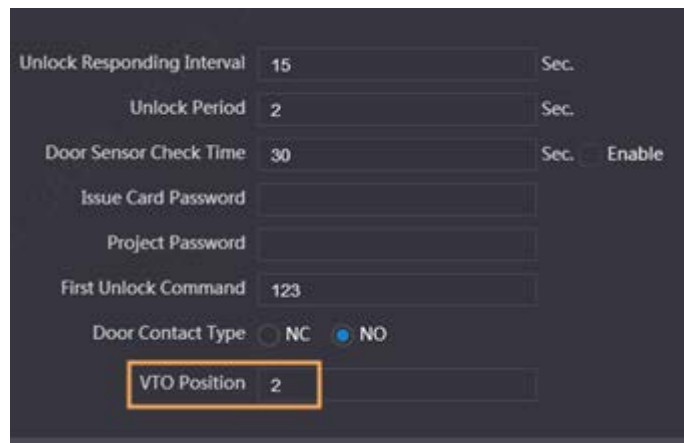


The screenshot shows a configuration window for 'LiftControl Enable'. At the top, there is a checked checkbox labeled 'LiftControl Enable'. Below it, there are several input fields: 'Index' is set to 'Lift 2' with a dropdown arrow; 'Enable' is a checked checkbox; 'IP Addr.' is a text field with a blurred IP address; 'Port' is set to '5000'; 'Username' is set to 'admin'; and 'Password' is a masked text field with six dots.

### Step 3 Configure VTO floor.

- 1) Select **Local Setting > Local**.
- 2) Configure **VTO Position**. For example, if the VTO is on the first floor, enter 1.
- 3) For configuring other parameters on the **Local** interface, see VTO user's manual.

Figure 5-8 Configure VTO floor



The screenshot shows a configuration window for VTO parameters. The parameters are: 'Unlock Responding Interval' (15 Sec.), 'Unlock Period' (2 Sec.), 'Door Sensor Check Time' (30 Sec.) with an 'Enable' checkbox, 'Issue Card Password' (empty), 'Project Password' (empty), 'First Unlock Command' (123), and 'Door Contact Type' (radio buttons for NC and NO, with NO selected). The 'VTO Position' field, containing the value '2', is highlighted with an orange box.

## 5.4 Configuring DSS Pro


### 5.4.1 Configuring Storage Disk

Add storage disks that can be used to store pictures and videos. You can add net disks and local disks.

### 5.4.1.1 Configuring Net Disk




- The storage server is required to be deployed.
- One user volume of the current net disk can only be used by one server at the same time.
- User volume is required to be formatted when adding net disk.

**Step 1** Log in to Web Manager, click , and then select **Storage**.

**Step 2** Select **Storage Config > Net Disk**.

**Step 3** Click **Add**.

**Step 4** Select server name, enter the IP address of net disk, and click **OK**.

- **User mode:** Enter the username and password of a disk user that has the permission of volumes on the net disk. Enable the user mode to add all the volumes of this user.
- **User mode disabled:** The platform shows the volumes not assigned to any user on the disk. The volumes in red are being used. To force to get it, click .




To force to get the disk, you need to format it. Data will be cleared after the disk is formatted. You are recommended to back up the data in advance.

Figure 5-9 Add net disk

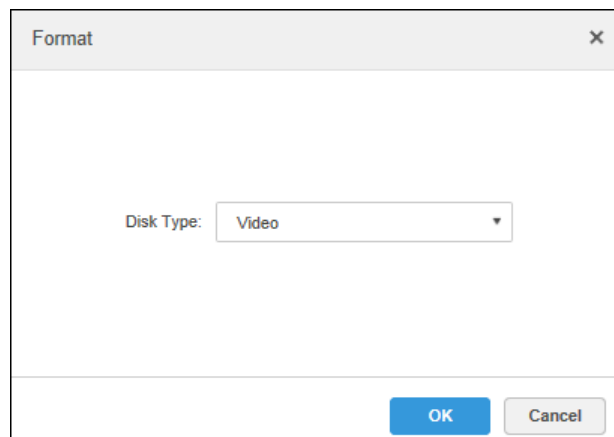
The screenshot shows a configuration form for adding a net disk. The fields are as follows:

- Server Name:** Center Server (dropdown menu)
- IP Address:** 1.1.1.1 (text input with a red asterisk indicating a required field)
- Enable User Mode:** ON (toggle switch with a blue 'ON' button and a warning icon)
- Username:** admin (text input with a red asterisk)
- Password:** [masked with dots] (password input with a red asterisk)

**Step 5** Select disk, click **Format** or click  next to the disk information to format the corresponding disk.

**Step 6** Select format disk type, and then click **OK**.


Figure 5-10 Format disk



**Step 7** Click **OK** in the prompt box to confirm formatting.

### 5.4.1.2 Configuring Local Disk

Configure local disk to store different types of files, including videos, ANPR snapshots, and face or alarm snapshots. In addition to the local disks, you can also connect an external disk to the platform server, but you have to format the external disk before using it.

**Step 1** Click , and then select **Storage**.

**Step 2** Select **Storage Config > Local Disk**.

**Step 3** Configure local disk.


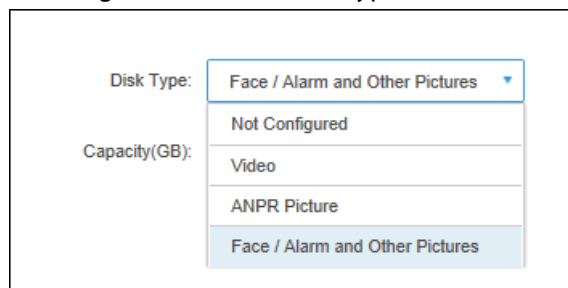

- Click  and configure disk type according to interface prompt.

Figure 5-11 Select disk type



- Select disk and click **Format**, or click  next to disk information and format the disk according to interface prompt and configure disk type.

## 5.4.2 Adding Devices

### 5.4.2.1 Manually Adding

**Step 1** Log in to the DSS Web Manager.

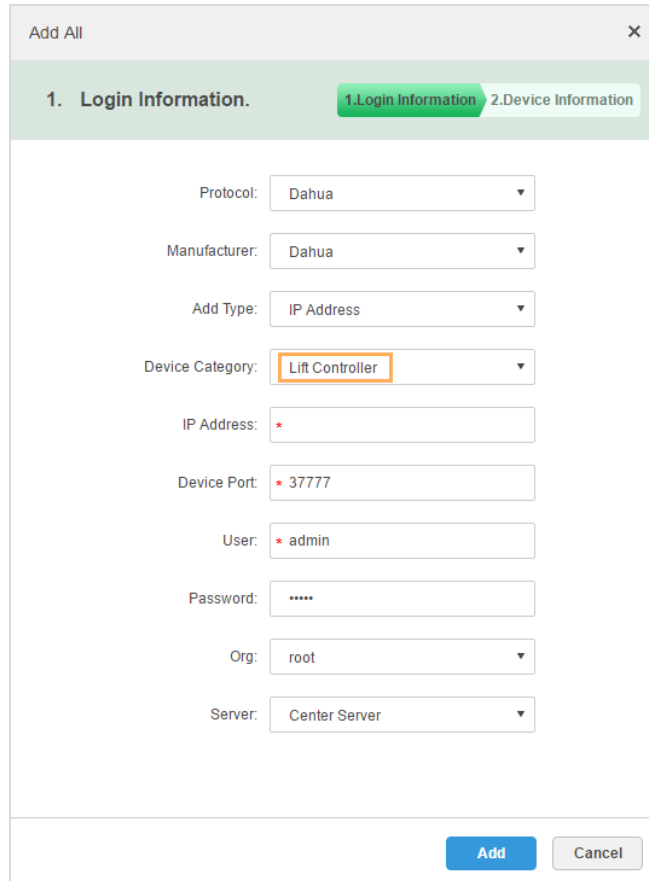
**Step 2** Click  and select **Device** on the **New Tab** interface.

Step 3 Click **Add**.

Step 4 Set parameters.

For **Device Category**, select **Lift Controller** for elevator controller, **Access Controller** for access controller, and **Video Intercom** for VTO, VTH and VTS.

Figure 5-12 Add a camera(1)



The screenshot shows a dialog box titled "Add All" with a close button (X) in the top right corner. It features two tabs: "1. Login Information" (which is active and highlighted in green) and "2. Device Information". The "1. Login Information" tab contains the following fields:

- Protocol: Dahua (dropdown menu)
- Manufacturer: Dahua (dropdown menu)
- Add Type: IP Address (dropdown menu)
- Device Category: Lift Controller (dropdown menu, highlighted with an orange border)
- IP Address: \* (text input field)
- Device Port: \* 37777 (text input field)
- User: \* admin (text input field)
- Password: \*\*\*\*\* (password input field)
- Org: root (dropdown menu)
- Server: Center Server (dropdown menu)

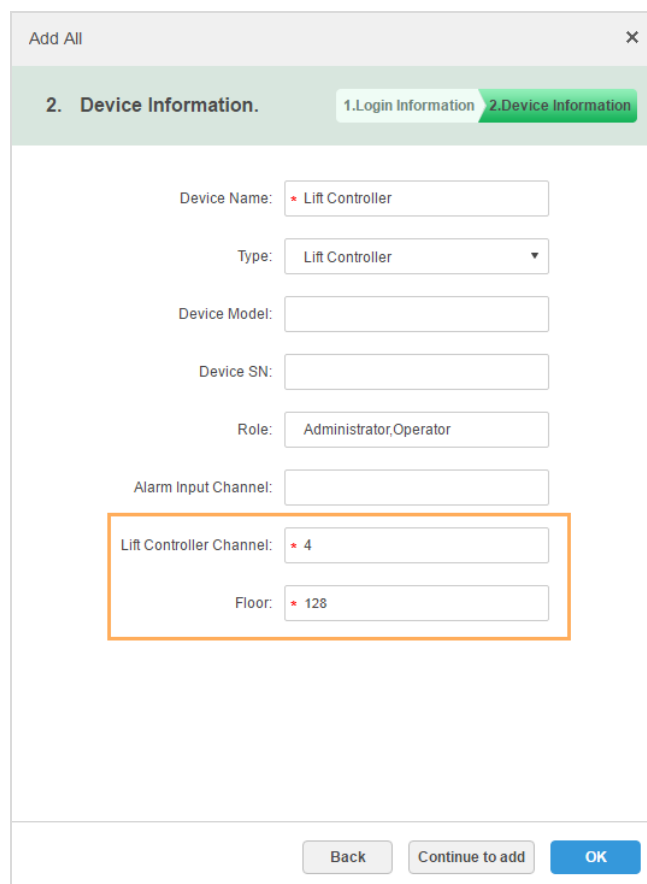
At the bottom right of the dialog, there are two buttons: "Add" (in blue) and "Cancel" (in grey).

Step 5 Click **Add**.

Step 6 Set the parameters.

Enter **Device Name**. For elevator controller, enter **Lift Control Channel** and **Floor** (number of floors).

Figure 5-13 Add a camera(2)



Step 7 Click **OK**.

### 5.4.2.2 Adding by Search

The platform automatically searches for and displays devices on the same network with DSS, so that you can quickly add devices from the search results.

Step 1 Click  and select **Device** on the **New Tab** interface.

Step 2 Click **Refresh** to search for online devices.

Step 3 Select a device, and then click **Connect**.




You can select multiple devices to add them in batches if they have the same username and password.



Figure 5-14 Batch add

Step 4 Set parameters, and then click **OK**.

### 5.4.2.3 Importing Video Intercom Device

Step 1 On the **Device** interface, click  [Imp...](#)

You can also export the template from Configtool.



The configuration of VTS is not included in the template exported from ConfigTool, you need to add VTS manually.

Figure 5-15 Import intercom device

Step 2 Click **Download Intercom Device Template** to download the template file.

- Step 3 Modify the file as you planned to modify IP addresses, assign SIP server, fence station and unit VTO, and also configure room numbers.
- Step 4 After modification, click **Import** to upload the template file, and then click **OK**.

### 5.4.3 Configuring Video Recording Plan

Step 1 Click  and select **Storage** on the interface of **New** tab.

Step 2 Click the **Record Plan** tab, and then click **Add**.

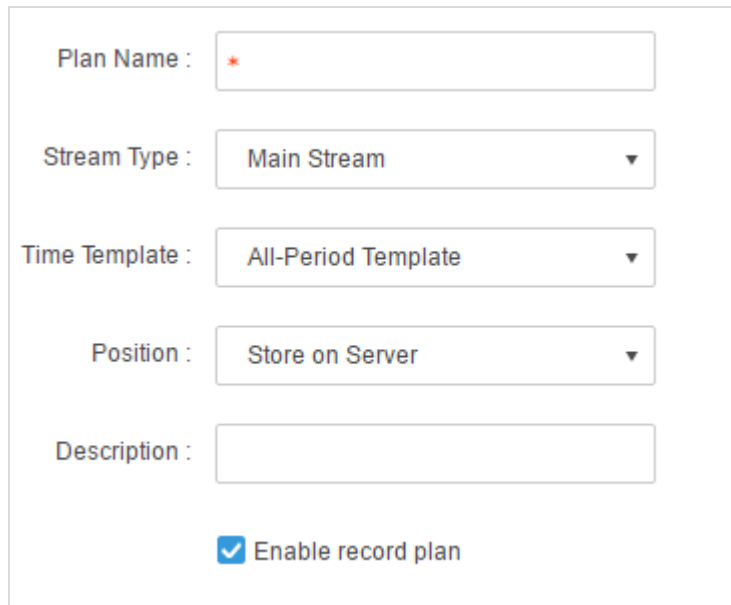
Step 3 Select a video channel, and then set parameters.



- Stream type: Select main stream, sub stream 1, or sub stream 2. The stream type selected here must be enabled on the device.
- Time template: Select the system default template or new template.
- Storage position: Select **Store on the Server** to store on the platform server disks; select **Store on Recorder** to store on the device.

Step 4 Click **OK**.

Figure 5-16 Add recording plan



### 5.4.4 Binding Video Channel to Elevator Controller

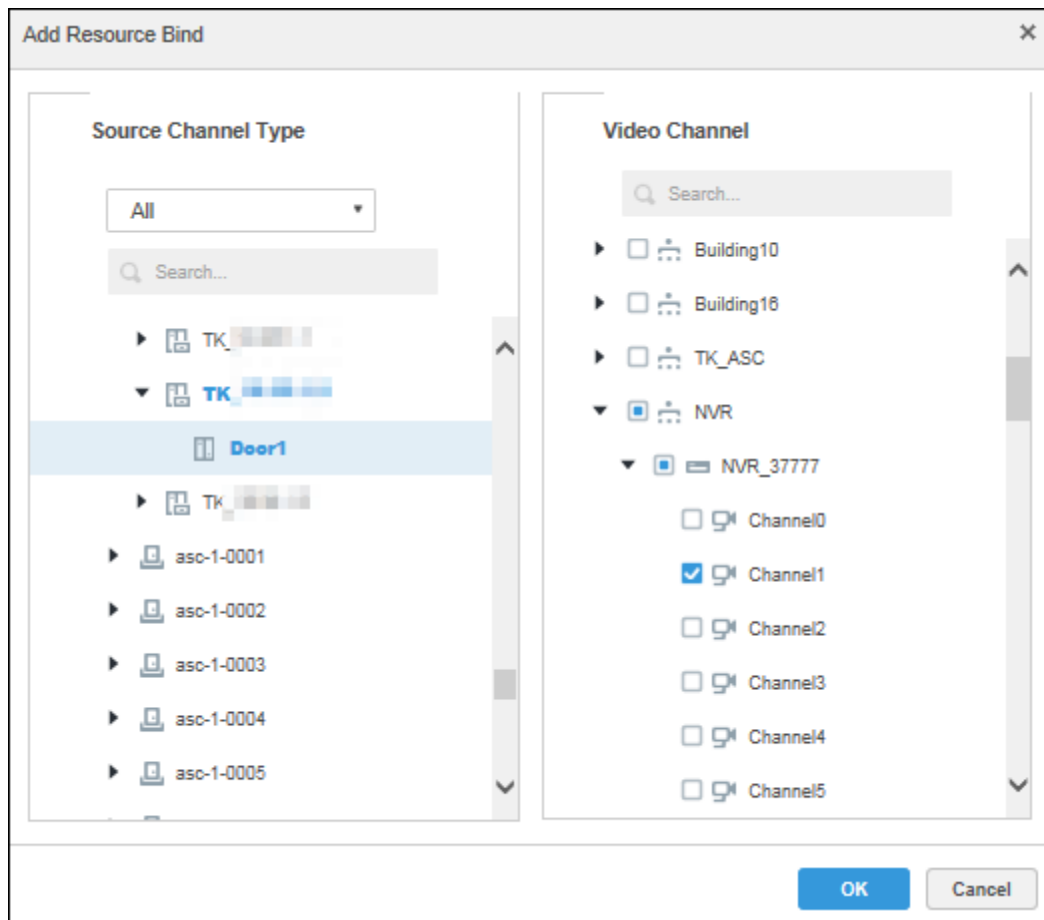
Bind cameras to elevator controllers so that you can check associated elevator videos when needed.

Step 1 Log in to the Web Manager. Click , and then select **Device**.

Step 2 Click **Resource Bind**.

Step 3 Click **Add**.

Figure 5-17 Add resource to bind




**Step 4** Select an elevator controller channel and the corresponding video channel respectively, and then click **OK**.

## 5.4.5 Configuring Access Permissions

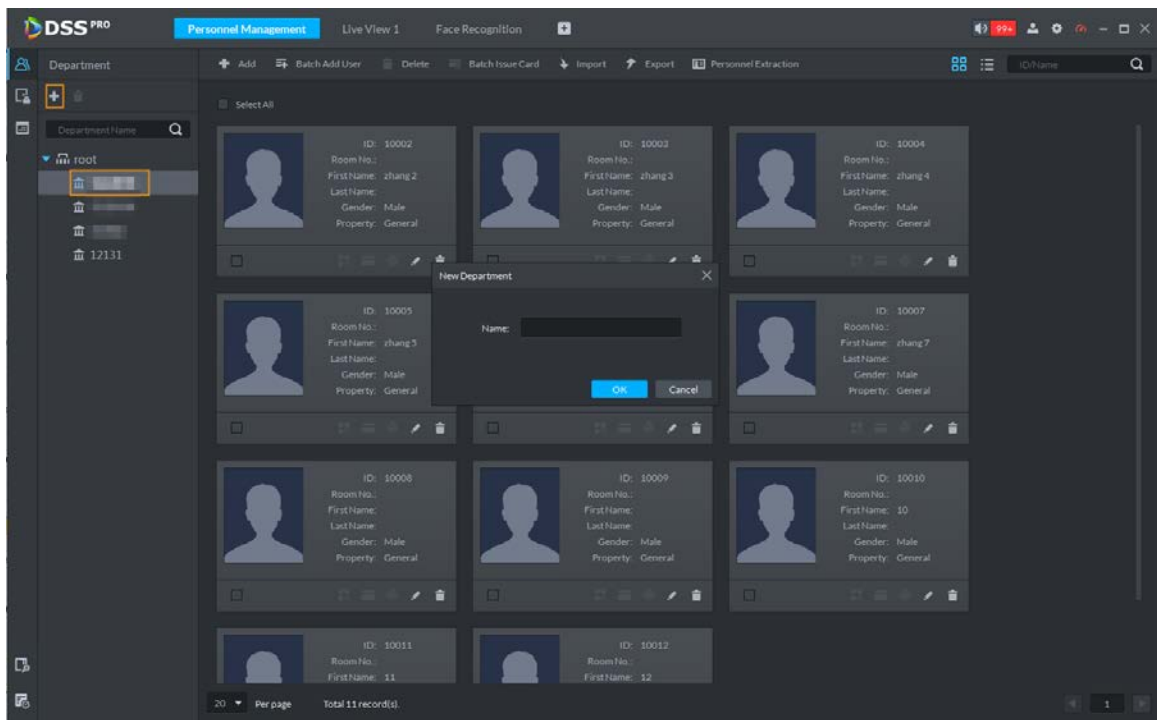
### 5.4.5.1 Adding Departments

Adding department is to manage personnel in the added departments.

**Step 1** Click  on the DSS Pro Client, and then select **Personnel Management**.

**Step 2** Select a node from the department list on the left side, and then click .

Figure 5-18 Add a department



**Step 3** Enter department name and click **OK**.

### 5.4.5.2 Adding Personnel and Authorizing

Add personnel, and then authorize access permissions. You can add personnel one by one or in batches.



- Person ID shall be the same on the platform and access control devices; otherwise person data could be wrong.
- To collect fingerprints or card No., connect a fingerprint collector or card reader first.

Face image requirements:

- Frontal view, shoulders shown, eyes open, looking forward, natural expression.
- No face masking such as hat, mask, and glasses. If there are two images for one person, the second image can be partially masked with mouth mask or glasses.
- Forehead shown, no fringe.
- Image size must be less than 75 KB, and the best pixel width is 200 px.

Figure 5-19 Proper image

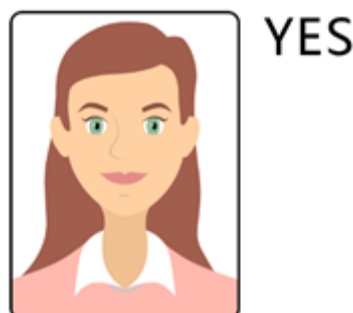


Figure 5-20 Improper images

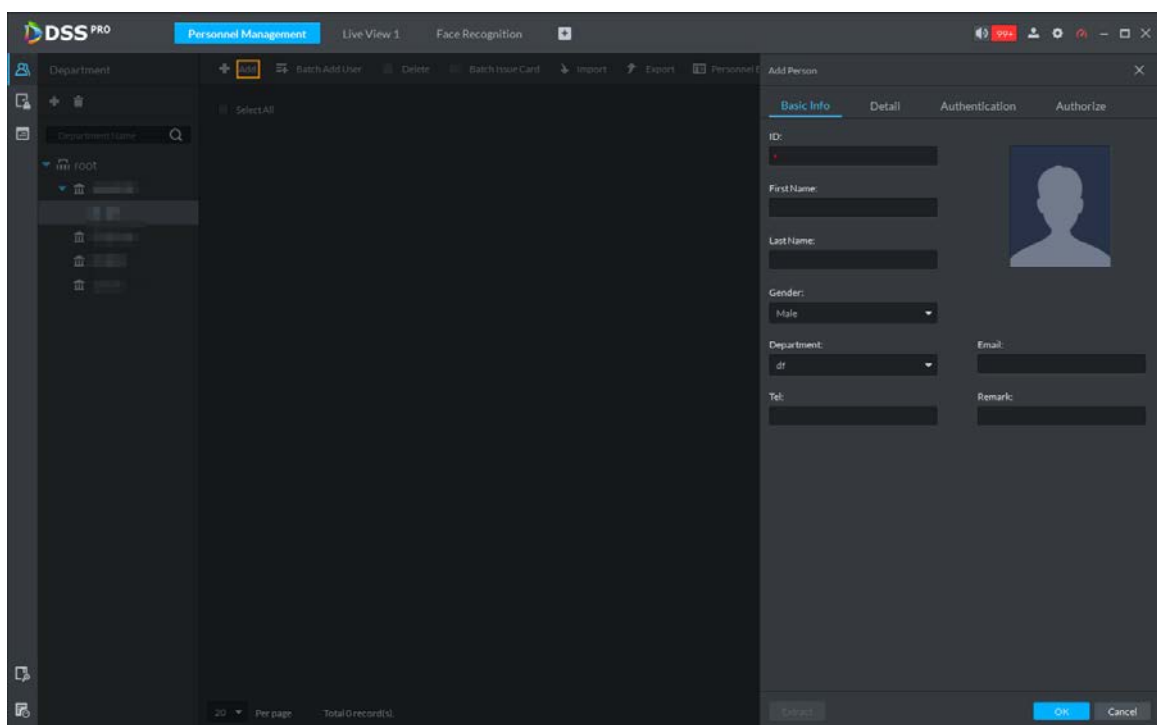


### 5.4.5.2.2 One by One

**Step 1** Log in to the DSS Pro Client, click , and then select **Personnel Management**.

**Step 2** Click **Add**.

Figure 5-21 Add a person



**Step 3** Click the **Basic Info** tab to configure person information.

- 1) Upload face image for face recognition.  
Point to the profile, and then click **Upload Picture** to select a picture or click **Snapshot** to take a photo.
- 2) Specify personnel information.  
ID is required and must be unique, and others are optional.

**Step 4** Click the **Detail** tab, and then set person details.

**Step 5** Click the **Authentication** tab, and then set validity period and access control information.

Figure 5-22 Authentication

The screenshot shows the 'Add Person' window with the 'Authentication' tab selected. The 'Validity' section contains 'Validity Time' (2020-03-11 00:00:00) and 'Expiration' (2030-03-11 23:59:59). The 'Access Control' section has 'Personnel Type' set to 'General' and 'Personnel Permission' set to 'User'. The 'Resident Information' section has 'Room No.' set to 'xxx#xxx#xxxxxx' and 'Householder' set to 'Off'. The 'Card' section has an 'Add' button and a warning icon with the text: 'Add card number to authorize personnel with permissions of devices beyond the second generation of access control device.' The 'Password' section has an 'Add' button and a warning icon with the text: 'The platform issues personnel password to second-generation access control devices, and issues card password to first-generation access control devices.' The 'Fingerprint' section has an 'Add' button, a 'Delete' button, and a table with columns 'Fingerprint Name' and 'Operation'. At the bottom are 'Extract', 'OK', and 'Cancel' buttons.

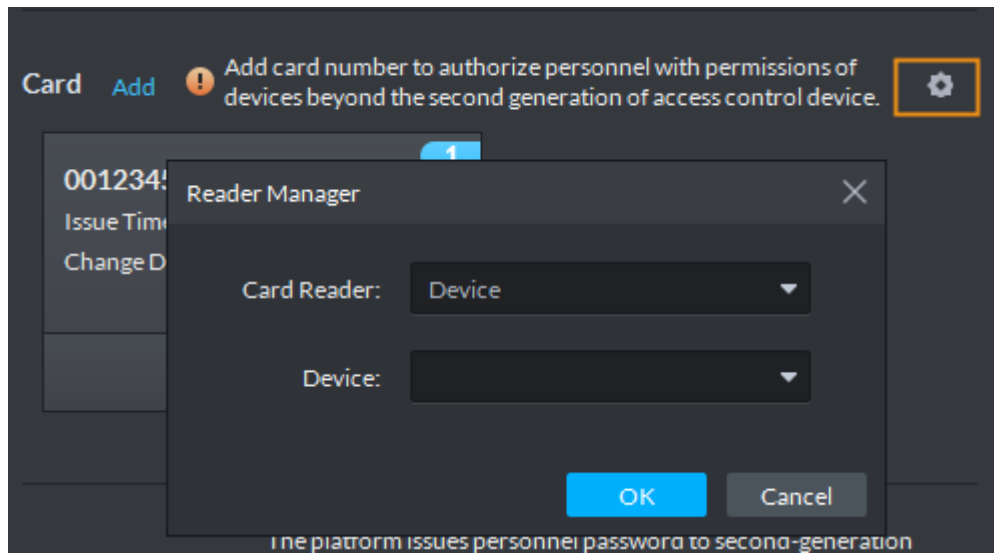
**Step 6** Issue card.

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 digits. 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 number 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 card reader

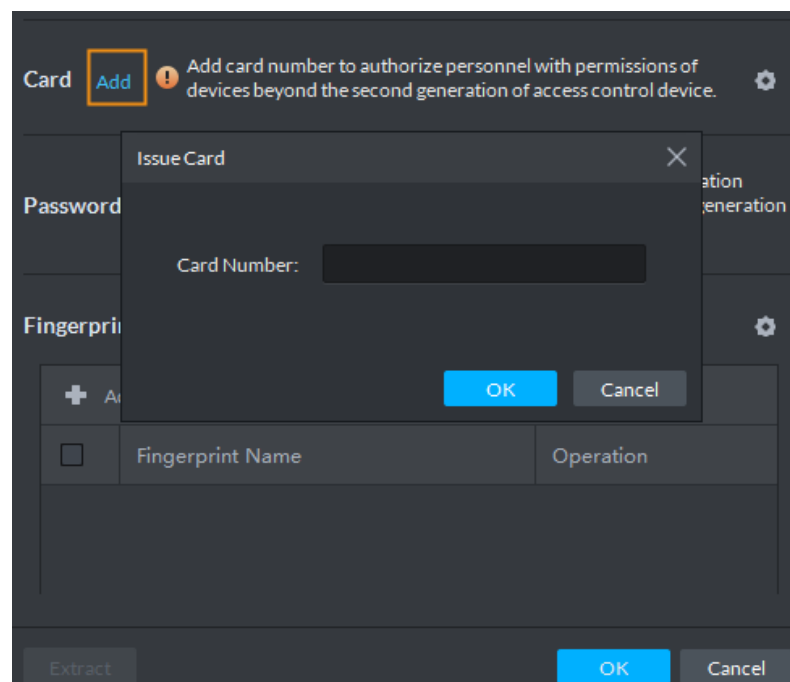
1) Click

Figure 5-23 Issue card by card reader



- 2) Select a reader from the **Card Reader** drop-down list or a device from the **Device** drop-down list, and then click **OK**.
- 3) Swipe card on the card reader or device.
  - By entering card No.
- 1) Click **Add** next to **Card**.

Figure 5-24 Issue card by entering card No.



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

Figure 5-25 Added card

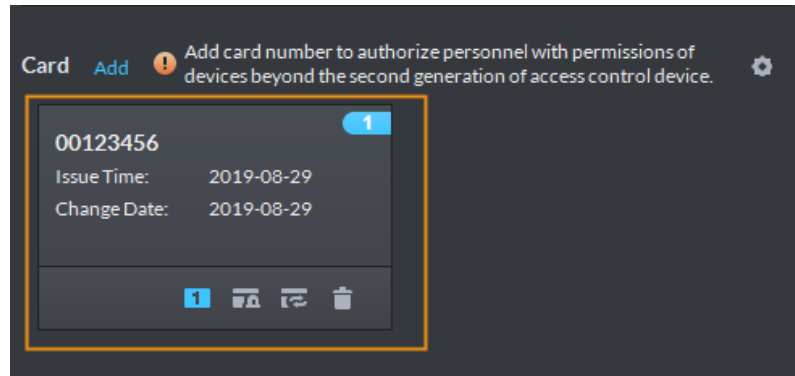


Table 5-2 Card operations

Icon	Description
	<p>If a person has more than one card, only the main card can be issued to the first-generation access control device. The first card of a person is the main card by default.</p> <p>Click  on an added card, the icon turns into , which indicates that the card is a main card. Click  to cancel the main card setting.</p>
	<p>Set a card as duress card. When opening door with a duress card, there will be a duress alarm.</p> <p>Click this icon, it turns into  and a  icon is displayed at upper right, which indicates that the card is set as a duress card. To cancel the duress setting, click .</p>
	<p>Change card for the person when the current card does not work.</p>
	<p>Remove the card, and then it has no access permission.</p>

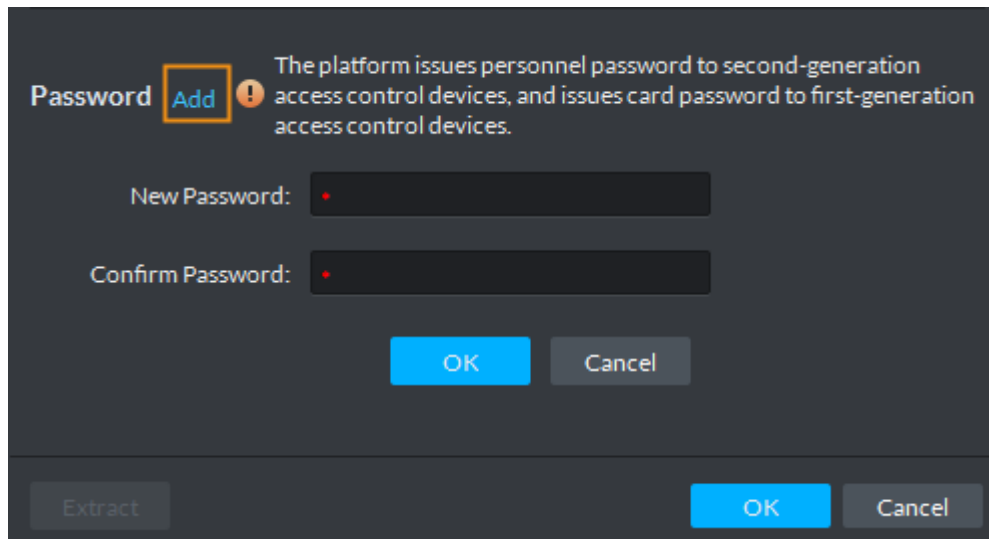
**Step 7** Set access password.

To open door with password, you need to set passwords for personnel, and then one can open door by entering person ID and password.

- 1) Click **Add** next to **Password**.



Figure 5-26 Set a password



2) Enter the password, and then click **OK**.

Figure 5-27 Added card

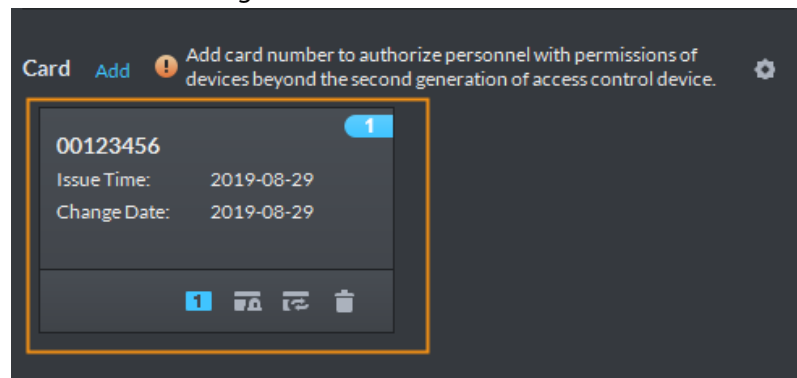


Table 5-3 Card operations

Icon	Description
	<p>If a person has more than one card, only the main card can be issued to the first-generation access control device. The first card of a person is the main card by default.</p> <p>Click  on an added card, the icon turns into , which indicates that the card is a main card. Click  to cancel the main card setting.</p>
	<p>Set a card as duress card. When opening door with a duress card, there will be a duress alarm.</p> <p>Click this icon, it turns into , and a  icon is displayed at upper right, which indicates that the card is set as a duress card. To cancel the duress setting, click .</p>
	Change card for the person when the current card does not work.
	Remove the card, and then it has no access permission.

### 5.4.5.2.3 In Batches

To quickly add a number of people, you can download a personnel template, fill in it and then import it to the platform.

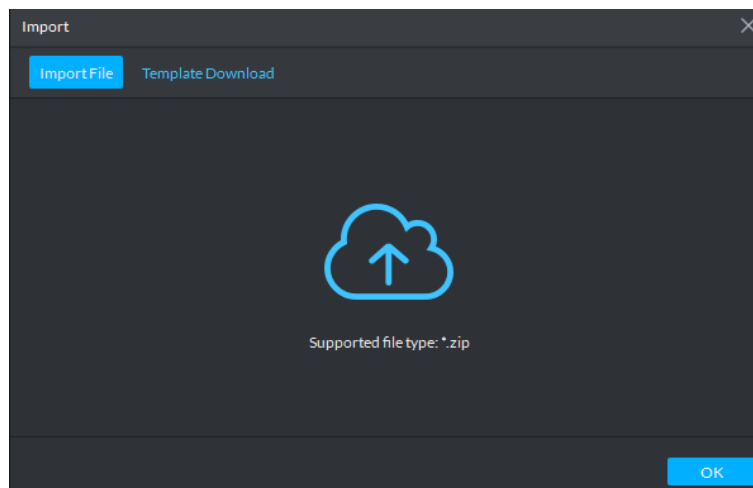


A personnel file shall be a zip package which includes an .xlsx file and face pictures, which supports up to 10000 pieces of person information. A personnel file shall not be larger than 1 GB.

**Step 1** Log in to the DSS Pro Client, click , and then select **Personnel Management**.

**Step 2** Click **Import**.

Figure 5-28 Import personnel information



**Step 3** Fill in personnel information template.

- 1) Click Template Download.
- 2) Fill in the template.  
In the template, face image name should be the same as that of the actual face image file of the person.
- 3) Zip the template excel and the face images into one file.

**Step 4** Click **Import File** to import the personnel information file.

**Step 5** Click **OK**.

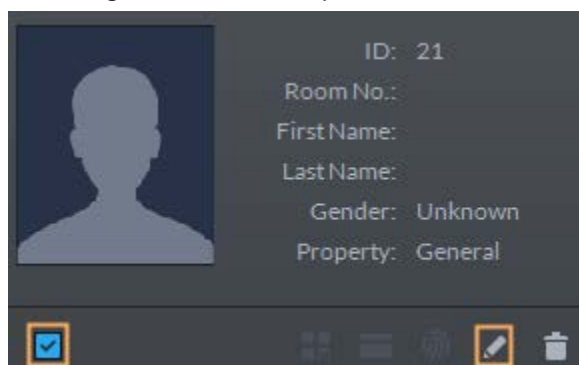


If there are failures, you can download the failures list to view details.

**Step 6** Configure VTO permissions.

- 1) Select a person by clicking , and then click .

Figure 5-29 Select a person

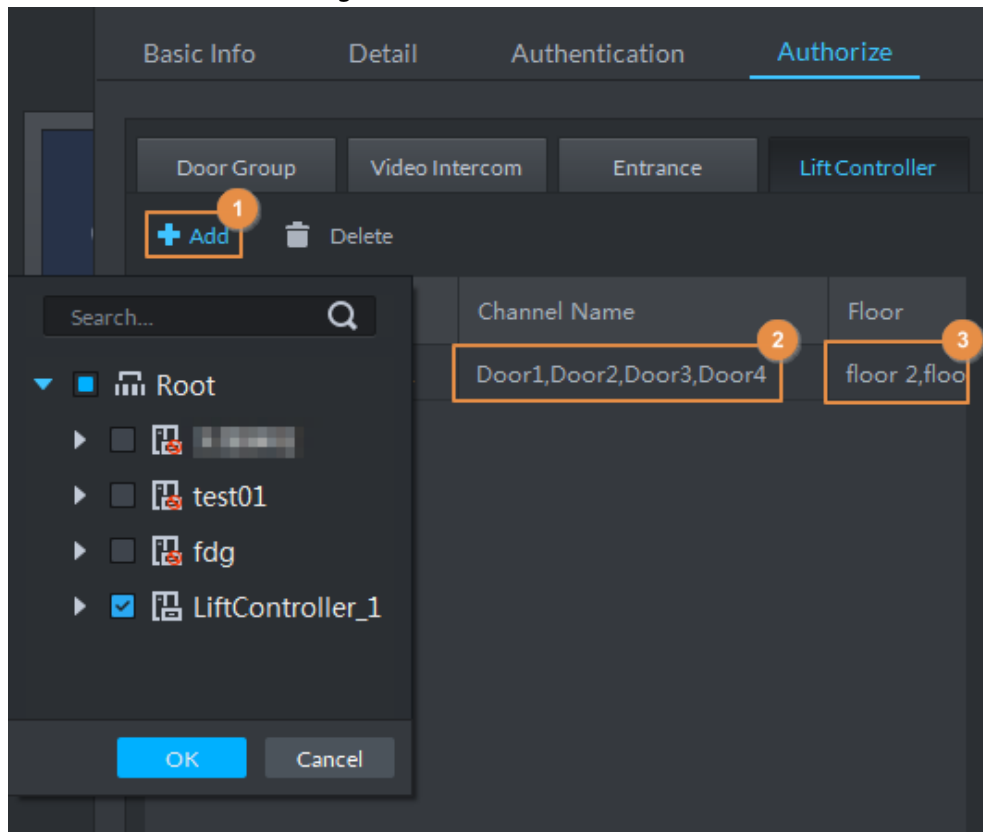


- 2) Select **Authorize > Video Intercom**.
- 3) Click **Select Room Number**, and then select the room No. of this person from the **Room No.** drop-down list.
- 4) Select **Authorize > Video Intercom**, and then select the VTO that this person can have access to.

Step 7 Configure elevator permissions.

- 1) Click **Authorize > LiftController**.
- 2) Click **Add**.
- 3) Select the elevator controller and floor that this person can have access to.

Figure 5-30 Authorize



- 4) Click **OK**.

Step 8 Repeat Step 4 to Step 5 to authorize all the newly added people one by one.

## 5.4.6 Configuring Elevator Control Event

Step 1 Log in to the DSS Pro Web Manager.

Step 2 Click **+** and select **Event** on the **New Tab** interface.

Step 3 Click **Add**.

Step 4 Select **Lift Controller**, and event type, **Lift Controller Authentication** for example.

Step 5 In **Alarm Source**, select devices.

Figure 5-31 Configure event

**Step 6** (Optional) Click **Alarm Linkage** to configure a linked action for the event. For details, see *DSS Pro User's Manual*.

**Step 7** Go back to the **Event** interface, click **OFF** to enable the event.

## 5.5 Commissioning

### 5.5.1 Calling Elevator from VTH

Tap **Call Elevator** or **Call Lift** on the VTH, and then check whether the elevator responds and comes to the floor of the VTH.

### 5.5.2 Opening Unit Door from VTH

Tap the unlock icon on the VTH, and then check whether the door is unlocked and the elevator comes to the floor of the VTO.

### 5.5.3 Calling Elevator from VTO

Swipe an authorized resident card on the VTO, and then check whether the door is unlocked and the elevator comes to the floor of the VTO.

# 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. 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.

#### **8. Assign Accounts and Privileges Reasonably**

According to business and management requirements, reasonably add users and assign a minimum set of permissions to them.

#### **9. 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.

#### **10. 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.

#### **11. 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.

#### **12. 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.

#### **13. 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.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.

ENABLING A SAFER SOCIETY AND SMARTER LIVING

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.

Address: No.1199 Bin'an Road, Binjiang District, Hangzhou, P. R. China | Website: [www.dahuasecurity.com](http://www.dahuasecurity.com) | Postcode: 310053

Email: [overseas@dahuatech.com](mailto:overseas@dahuatech.com) | Fax: +86-571-87688815 | Tel: +86-571-87688883