MPT Manager

User Manual

Foreword

This manual introduces the functions and operations of the MPT Manager PC client (hereinafter referred to as "the client").

Safety Instructions

The following signal words might appear in the manual.

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.
TIPS	Provides methods to help you solve a problem or save time.
NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	June 2025

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, audio, fingerprints, and license plate number. You need to be in compliance with your local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures which include but are not limited: Providing clear and visible identification to inform people of the existence of the surveillance area and provide required contact information.

About the Manual

- The manual is for reference only. Slight differences might be found between the manual and the product.
- We are not liable for losses incurred due to operating the product in ways that are not in compliance with the manual.
- The manual will be updated according to the latest laws and regulations of related jurisdictions. For detailed information, see the paper user's manual, use our CD-ROM, scan the QR code or visit our official website. The manual is for reference only. Slight differences might be found between the electronic version and the paper version.
- All designs and software are subject to change without prior written notice. Product updates might result in some differences appearing between the actual product and the manual. Please contact customer service for the latest program and supplementary documentation.
- There might be errors in the print or deviations in the description of the functions, operations and technical data. If there is any doubt or dispute, we reserve the right of 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 company names in the manual are properties of their respective owners.
- Please visit our website, contact the supplier or customer service if any problems occur while using the device.
- If there is any uncertainty or controversy, we reserve the right of final explanation.

Table of Contents

1 Overview

MPT Manager, a computer client software, provides services, such as audio and video export backup, log export, and device upgrade, supporting handheld devices such as MPT320, body camera N1 and so on. This manual takes MPT230 as an example.

Before using the software, make sure that the Android drivers are installed on your computer and that it can recognize the individual device properly.

2 Basic Settings

2.1 Device Connection

Procedure

Step 1 Install the MPT Manager.

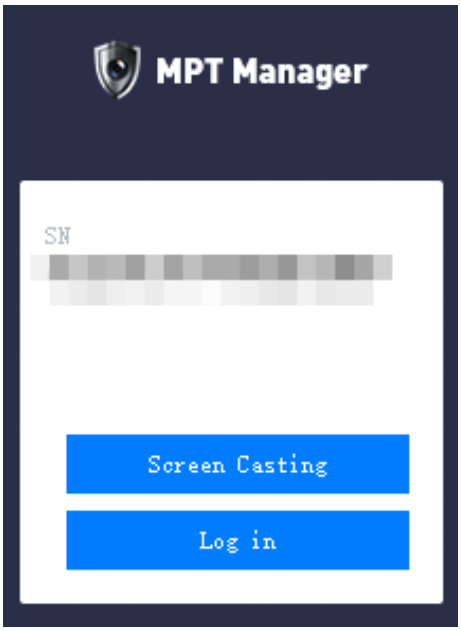
Follow the system prompts and click **Next** until the installation is complete. After that, a shortcut icon for MPT Manager will be displayed on your computer desktop.

Step 2 Start the Device, and then connect it to your computer through the USB cable.

Step 3 Double-click  on the desktop, click **Log in** to enter device password, and then click **OK**.

When the computer detects the device, it will display the device's serial number on the left side.

Figure 2-1 Log in to MPT Manager

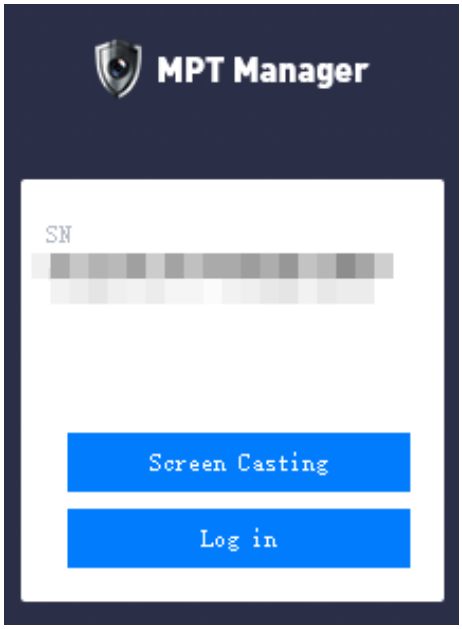


2.2 Screen Casting

You can perform screen casting for the MPT 230 and body camera N1 on your computer.

After you connect the device to the computer, click **Screen Casting** to project the device's interface on the computer, enabling remote control of the device through the computer.

Figure 2-2 Log in to MPT Manager



The device's logging in and screen casting cannot be enabled at the same time.

2.3 Device Management

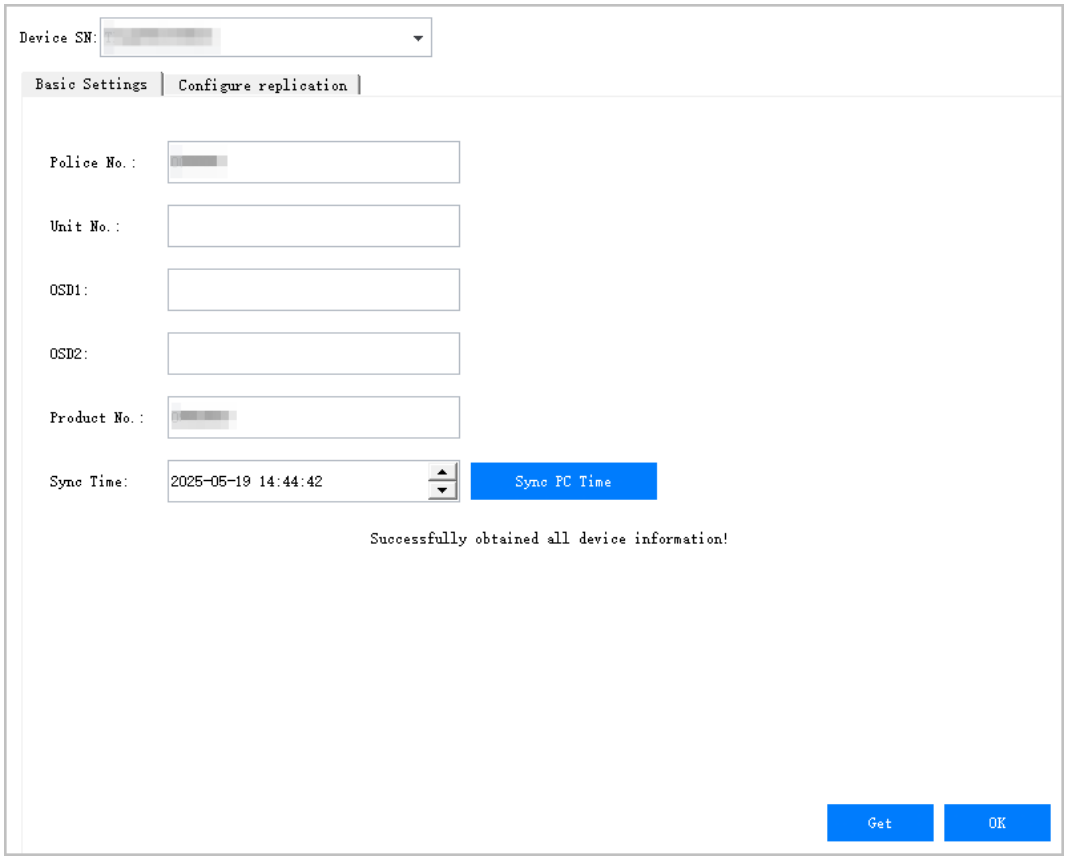
Procedure

Step 1 After you connect the device to the computer and log in to the MPT Manager, click **Setup**.

Step 2 Select the corresponding device SN number from the drop-down list to select the device.

Step 3 In the **Basic Settings** tab, click **Get** to obtain the device information.

Figure 2-3 Device management



Click **Sync PC Time** to synchronize the device's time with the computer's time.

2.4 Device Replication

You can copy the active registration and coding configurations, but the registration ID has been replaced with the same value and you need to manually adjust it.

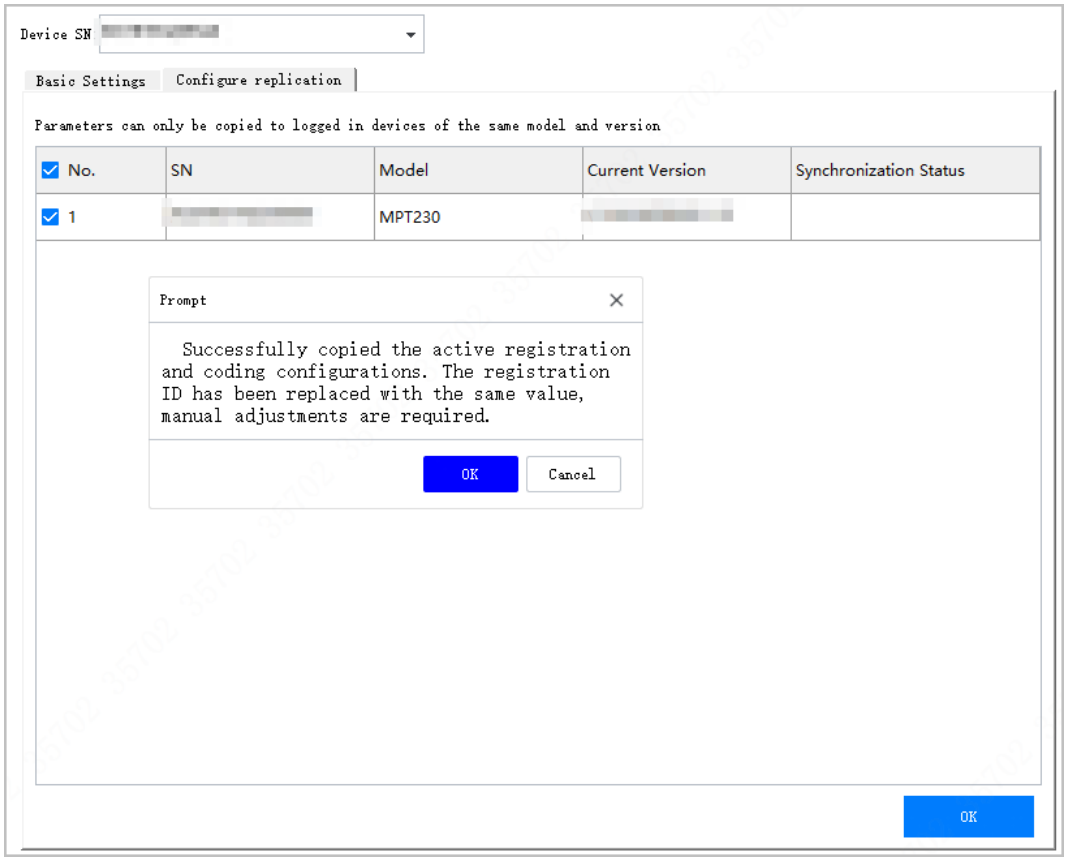
Procedure

Step 1 Connect at least two MPT devices to the computer, and then select **Setup** > **Configure replication** to enter the replication page.

Parameters can only be copied to logged-in devices of the same model and version.

Step 2 Select the device you want to copy information to in the list and click **OK** in the pop-up window.

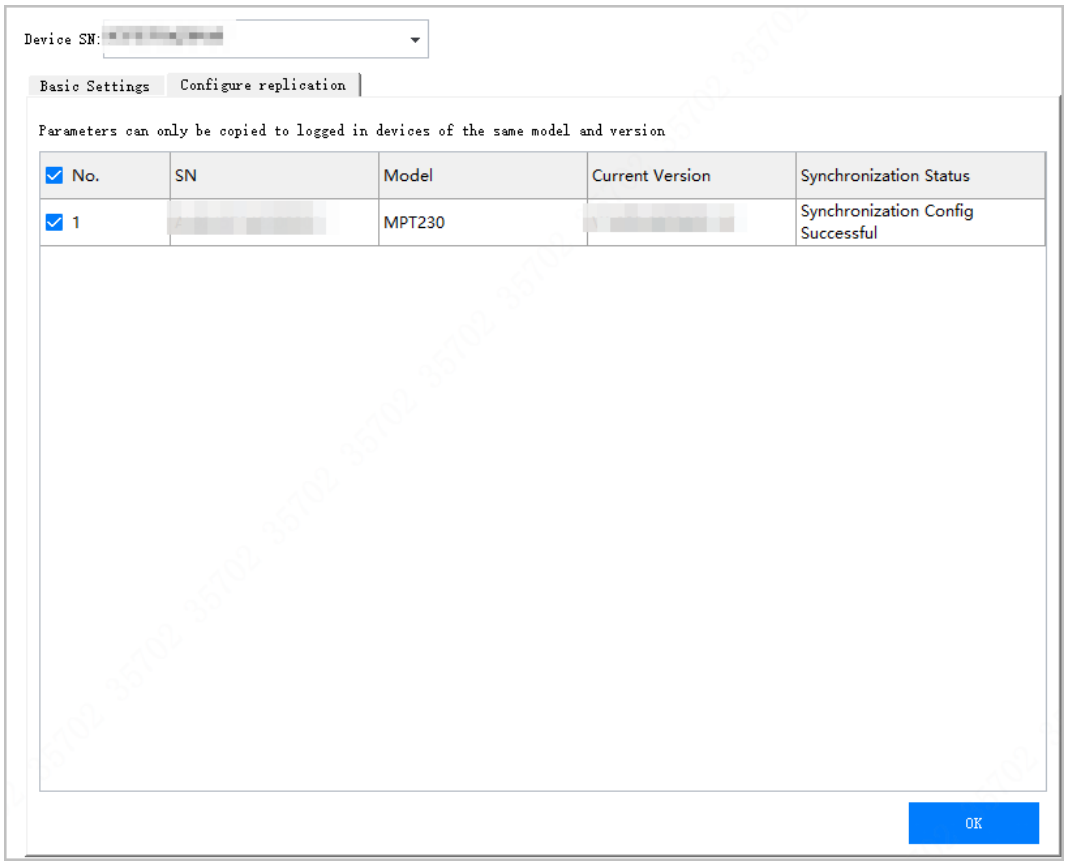
Figure 2-4 Replicate the settings



Results

The synchronization status prompts "**Synchronization Config Successful** ".

Figure 2-5 Success prompt

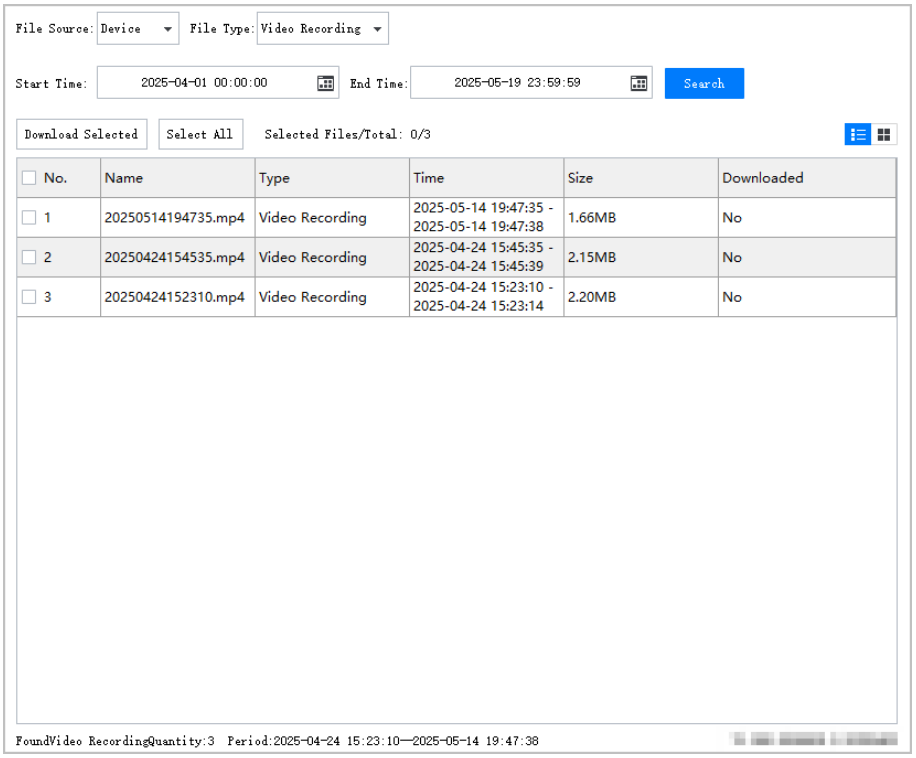


3 File Export Backup

You can back up the connected devices' files by the way of copying or cutting.

1. After you connect the device to the computer and log in to the MPT Manager, click **File**.

Figure 3-1 File export backup



2. Click  at the upper-right corner to configure the storage management settings, and then click **OK**.

Figure 3-2 Storage management

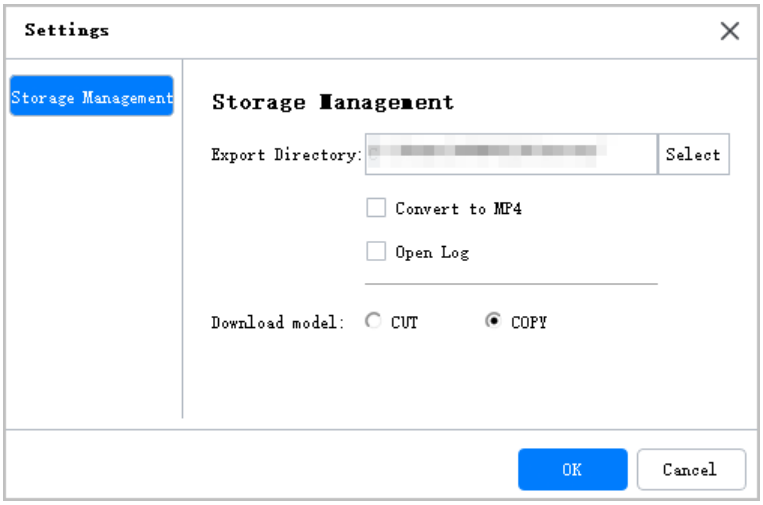


Table 3-1 Description of storage management parameters

Parameter	Description
Export Directory	Select the location on your computer where you want to back up.
Convert to MP4	If you back up a video, selecting this will automatically convert it to MP4 format.
Open Log	If you select it, the backing up process will automatically open the logs.
Download model	• **CUT** : Backing up process will delete the files in the device automatically. • **COPY** : Backing up process will not delete the files in the device.

3. Select the file source, file type, start time and end time, and then click **Search**.
4. Select the files you want to back up and click **Download Selected** to download them in the computer.

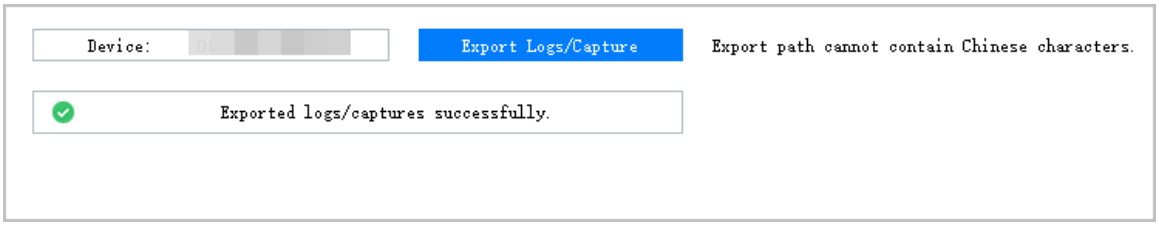
Click **Select All** to select all files in the search result.

4 Log Export and Packet Capture

You can export logs and perform packet capture for the device.

1. After you connect the device to the computer and log in to the MPT Manager, click **Log**.

Figure 4-1 Log export and capture



2. Click **Export Logs/Capture** to start the process.

   When this process is successful, it will prompt **Exported logs/captures successfully**.

5 Device Upgrade

You can upgrade the device through MPT Manager.

1. After you connect the device to the computer and log in to the MPT Manager, click **Upgrade**.
2. Click **Upgrade** to enter the upgrade page and select the update mode from the drop-down list.

Figure 5-1 Device upgrade

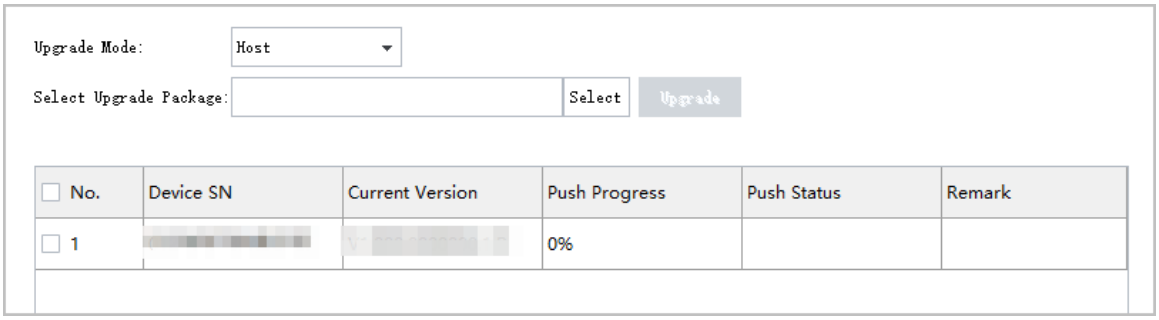
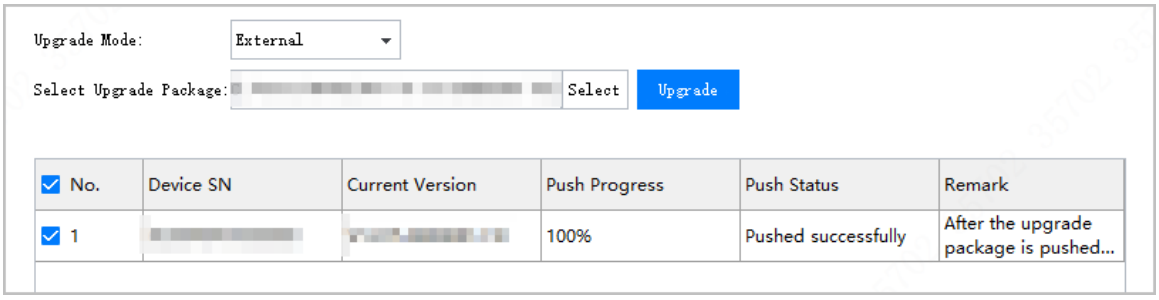


Figure 5-2 Successful push status



3. Click **Select** to select the upgrade package and click **Upgrade**.
4. Select the device and click **Upgrade**.

   The push progress becomes 100% when the update package is successfully pushed to the Device.

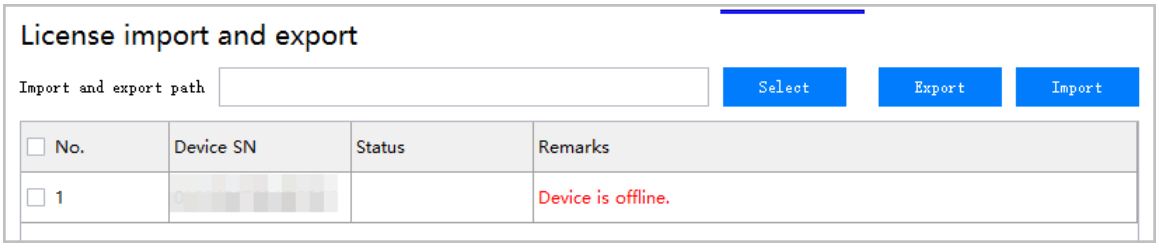
6 License Import and Export

You can import and export the device's license.

1. After you connect the device to the computer and log in to the MPT Manager, click **License**.
2. License Import and Export.

- Import the device license: Click **Select** to select the license import path, click ☐ to select the devices that you want to perform operations, and then click **Import**.
- Export the device license: Click **Select** to select the license export path, click ☐ to select the devices that you want to perform operations, and then click **Export**.

Figure 6-1 License import and export



Appendix 1 Security Recommendation

1. **Account Management**
   a. **Use Strong 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.

   b. **Change Password Regularly**

      It is suggested to change passwords regularly to reduce the risk of being guessed or cracked.

   c. **Assign Accounts and Permissions Reasonably**

      According to business and management needs, reasonably add new users, and reasonably allocate a minimum set of permissions for them.

   d. **Enable Account Lock**

      The account lock feature is enabled by default, and it is recommended 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.

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

      The platform supports password reset function. To reduce the risk of being attacked, please set up related information for password reset in time. 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.

   f. **Enable Account Binding IP/MAC**

      It is recommended to enable the account binding IP/MAC mechanism to further improve access security.

2. **Service Configuration**
   a. **Enable HTTPS**

      It is suggested to enable HTTPS, so that you visit web service through a secure communication channel.

   b. **Disable Unnecessary Services and Choose Secure Modes**

      If not needed, it is recommended to turn off some services such as SNMP, SMTP, etc., to reduce risks.

      If necessary, it is highly recommended that you use safe modes, including but not limited to the following services:

      - SMTP: Choose TLS to access mailbox server.
      - FTP: Choose SFTP, and set up strong passwords.

3. **Network Configuration**
   a. **Enable Firewall Allowlist**

      It is suggested to enable allowlist 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 allowlist.

   b. **Network Isolation**

The network should be isolated by partitioning the video monitoring network and the office network on the switch and router to different VLANs. This prevents attackers from using the office network to launch Pivoting attacks on the video monitoring network.

4. **Security Auditing**

   a. **Check Online Users**

      It is recommended to check online users irregularly to identify whether there are illegal users logging in.

   b. **View the Platform Log**

      By viewing the log, you can get the IP information of the attempt to log in to the platform and the key operation information of the logged-in user.

5. **Physical Protection**

   It is suggested to perform physical protection to the device that has installed the platform. For example, place the device 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.

6. **Perimeter Security**

   It is suggested to deploy perimeter security products and take necessary measures such as authorized access, access control, and intrusion prevention to protect the software platform security.