

Data Collection Station

User Manual



V1.0.1

Foreword

General

This manual introduces the functions and operations of the data collection station (hereinafter referred to as "the Station"). Read carefully before using the whiteboard, and keep the manual safe for future reference.

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.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
 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
V1.0.1	Updated some descriptions	December 2025
V1.0.0	First release.	July 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 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.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the whiteboard, hazard prevention, and prevention of property damage. Read carefully before using the whiteboard, and comply with the guidelines when using it.

Transportation Requirements



Transport the device under allowed humidity and temperature conditions.

Storage Requirements



Store the device under allowed humidity and temperature conditions.

Installation Requirements



- Do not install the device in a place exposed to sunlight or near heat sources.
- Keep the device away from dampness, dust, and soot.
- Install the device on a stable surface to prevent it from falling.
- Install the device in a well-ventilated place, and do not block its ventilation.

Operation Requirements



- Use the standard power adapter. We will assume no responsibility for any problems caused by the use of a nonstandard power adapter.
- Use the power cords that are recommended for the region and conform to the rated power specifications.
- Make sure all cables are connected correctly before plugging the whiteboard into the power. Do not overload the power socket or pull the power cord. Otherwise, it might cause fire or electric shock.



- Do not drop or splash liquid onto the device, and make sure that there is no object filled with liquid on the device to prevent liquid from flowing into it.
- Operate the device within the rated range of power input and output.
- The power supply must conform to the requirements of ES1 in IEC 62368-1 standard and be no higher than PS2. Please note that the power supply requirements are subject to the device label.
- Use the device under allowed humidity and temperature conditions.

- The device is a class I electrical appliance. Make sure that the power supply of the device is connected to a power socket with protective earthing.

Maintenance Requirements



Do not disassemble the device without professional instruction.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Introduction.....	1
1.1 Dimensions.....	1
1.2 Ports.....	1
1.3 Power on.....	2
2 HDD Installation.....	3
3 Configuration and Operation.....	5
3.1 Local Configuration.....	6
3.1.1 Device Initialization.....	6
3.1.2 Login.....	7
3.1.3 Password Reset.....	8
3.1.4 File Management.....	9
3.1.5 Searching for Logs.....	11
3.1.6 Local Settings.....	13
3.2 Web Configuration.....	44
3.2.1 Device Initialization.....	44
3.2.2 Login.....	45
3.2.3 File Management.....	46
3.2.4 Log.....	48
3.2.5 Settings.....	51
Appendix 1 Security Recommendation.....	55

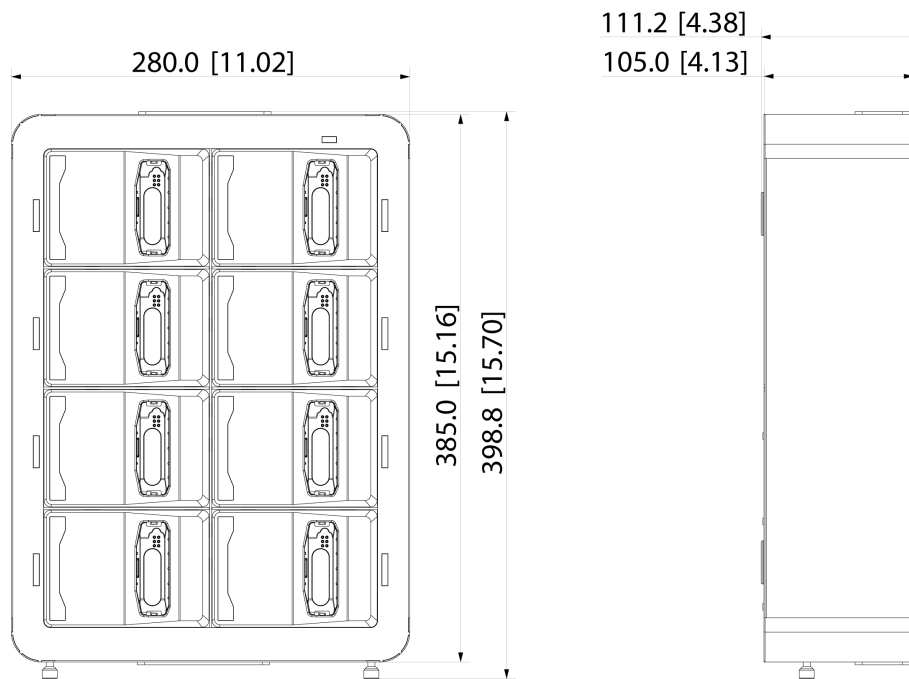
1 Introduction

Working with body camera, the Station can acquire the data of body cameras and charge them. The Station can automatically recognize and connect the body camera through the USB port. Working with the platform, the Station can authorize the body camera, automatically acquire the electronic evidence (video, audio, and snapshots). It is featured with:

- Recharge and collect data from maximum 8 body cameras at the same time.
- Automatically or manually upgrade body cameras.
- Automatically archive the collected electronic data.
- Automatically upload the evidence to FTP or the platform.
- Automatically synchronize time.
- You can search, edit, transcode, play back, view, delete, flag the file, and manage all the data in the Station.

1.1 Dimensions

Figure 1-1 Dimensions of EEC400-D (mm [inch])



1.2 Ports

Figure 1-2 Ports of EEC400-D (1)

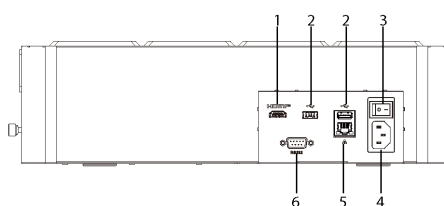


Figure 1-3 Ports of EEC400-D (2)

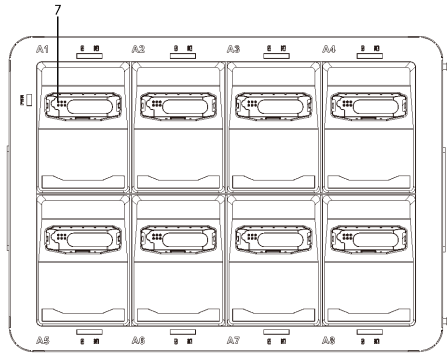


Table 1-1 Ports description

No.	Name	Description
1	HDMI port	Inputs uncompressed high definition (HD) video signals and multichannel audio signals from the external HDMI sources. Supports 1080p@60 Hz.
2	USB ports	Connects to USB storage devices (USB 2.0 and USB 3.0) and mouse.
3	Power switch	Turn on or turn off the Station.
4	Power input	220 VAC, power input for the Station.
5	Network port	Gigabit Ethernet port.
6	RS-232 port	Used for common serial debugging, IP address configuration and data transmission of transparent serial.
7	Pogo pin	Pin connector, used for connecting the MPT.

1.3 Power on

Procedure

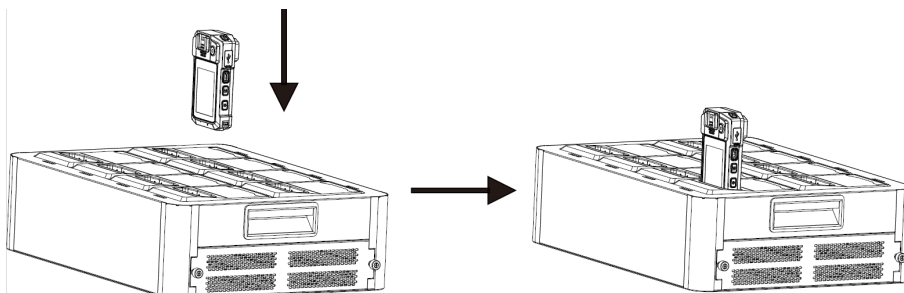
Step 1 Connect the power cable, network cable and HDMI.

Step 2 Press the power button.

The whole process will take a period of time. Please be patient.

Step 3 Align the charging port of the MPT with the pins in the slot of the Station and insert the MPT smoothly.

Figure 1-4 Connect to the device



2 HDD Installation

You can install 4 HDDs (hard disk drives).



The Station supports connecting the peripheral with magnets. The peripheral must be placed correctly. If the peripheral with magnet is placed in the air outlet of the Station, the fan will be attracted by the magnet and stop working.

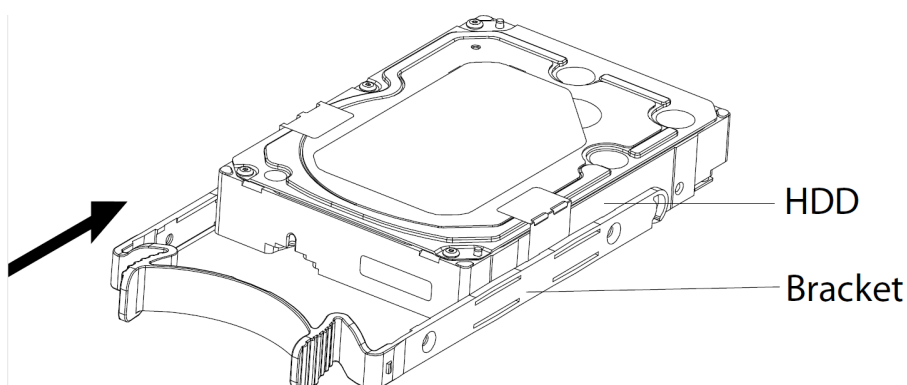


- To avoid insufficient storage space, HDDs larger than 2 TB are recommended.
- To reduce the writing pressure of each HDD, we recommend you install at least 2 HDDs with the same capacity for data collection and recharging.

Procedure

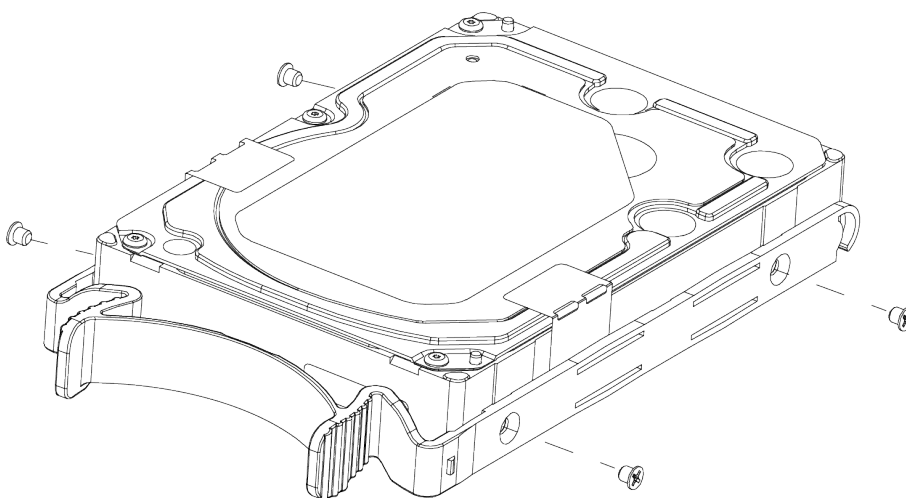
Step 1 Put the bracket flat on the desktop, and then install the HDD horizontally into the bracket.

Figure 2-1 Install the HDD



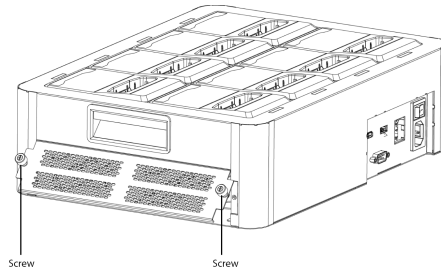
Step 2 Tighten the 4 screws on the bracket.

Figure 2-2 Tighten the screws



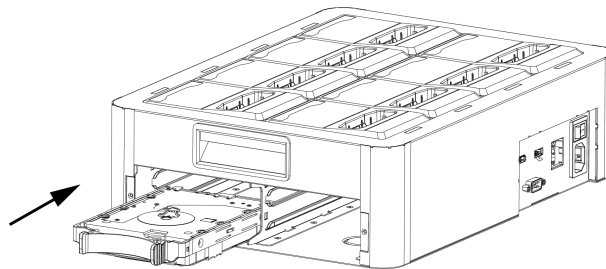
Step 3 Loosen the following screws to the leftward, and then hold the screws and rotate them outward to detach the cover.

Figure 2-3 Detach the cover



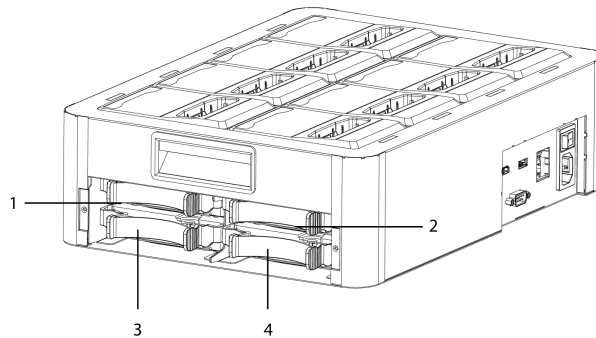
Step 4 Push the HDD with bracket installed into the chassis guide rails.

Figure 2-4 Install the bracket to the chassis



Step 5 (Optional) Repeat step 1, step 2, step 3 and step 4 to add more HDDs.

Figure 2-5 4 HDDs installation



Step 6 Hold the screws and rotate them inward to insert them into the screw holes in the chassis, and then tighten the screws to the rightward.

3 Configuration and Operation

Figure 3-1 Home screen

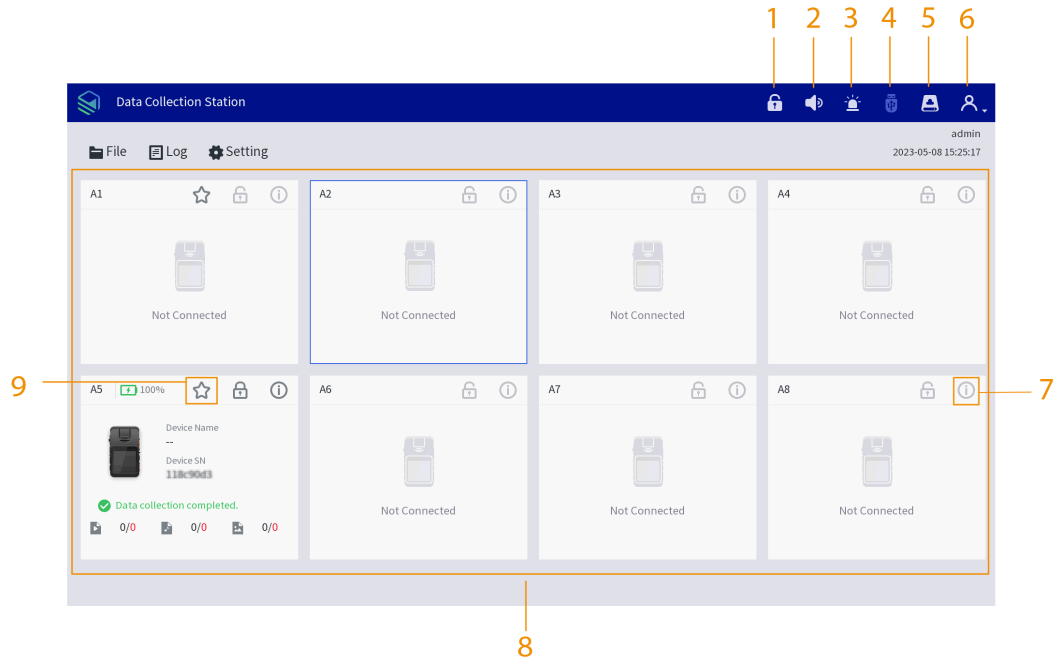


Table 3-1 Home screen description

No.	Description
1	Unlock the Station with one tap. And then you can remove the body camera.  Click  on a different body camera's page to unlock the specific body camera.
2	Alarm. Tap it, and the alarm tune is turned off.
3	Alarm information display. The red light flashes when there is alarm.
4	External USB storage device. ● Grey means no data is being exported. ● Green means data of selected body camera is exporting.
5	View HDD capacity.
6	Login, logout, restart, shutdown, and editing the user information.

No.	Description
7	When the Station is in a logged-in state and connected to body cameras, it supports viewing the information of body cameras, modifying their main account password, copying configuration parameters between body cameras, and accessing upgrade information for the Station. - Click Bind Enforce on the Device Info page, enter the enforcer name and enforcer No, click Search, and then select the enforcer that you want to bind. Click  to unbind the device. - Supports to check the update information. You can upload the update package in Maintain > Manager > Update to update the device. For details, see the corresponding user manual. In the configuration management page, click Copy To. In the pop-up selection page, select the corresponding slot number to copy the configuration parameters of the current slot recorder to the selected slot recorder. In the configuration management page, enter the new password in the Change Password and Confirm Password fields. Click OK to update the password for the current slot's recorder.
8	Displays the connected devices.
9	 indicates collecting data in priority, which can improve the collecting speed of the corresponding dock.  To enable this function, you need to connect at least two data collection modules. The function is supported by the two docks of the first row in each data collection module.

3.1 Local Configuration

3.1.1 Device Initialization

When booting up for the first time, you need to configure the username (admin by default) and password of the administrator.



For account security, we recommend keeping the password properly and change it regularly.

Procedure

- Step 1 Power on the device.
- Step 2 Select the region, language, and then click **Next**.
- Step 3 Read **Software License Agreement** and **Privacy Policy**, click **I have read and agree to the terms of the Software License Agreement and Privacy Policy.**, and then click **Next**.
- Step 4 Set the time zone and system time as needed, and then click **Next**.

Step 5 Configure the admin password, confirm it, and then click **Next**.

Figure 3-2 Set password

Step 6 Set security questions, and then click **Next**.



- After you set password protection, if you forget the admin login password, you can reset it using your registered phone number or security questions. For detailed instructions on how to reset the password, see "3.1.3 Password Reset".
-

You can reset the admin password by reserved email or security question. For details, see "3.1.3 Password Reset".

Step 7 Set the date and time, and then click **Next**.

Step 8 Click  to modify the IP address, and then click **Next**.

The initialization is finished.

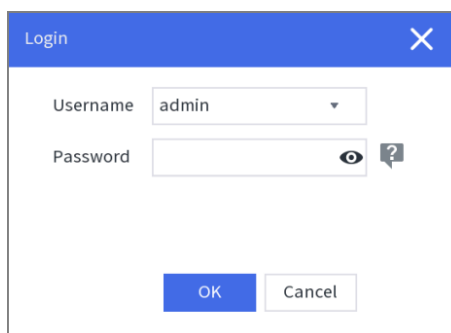
Figure 3-3 TCP/IP

3.1.2 Login

Procedure

- Step 1** Turn on the device.
- Step 2** Click  on the upper-right corner.
- Step 3** Enter the username and password, and then click **OK** to log in.

Figure 3-4 Login

A login dialog box with a blue header bar containing the text "Login" and a close button (X). The main area is white and contains two input fields: "Username" with a dropdown menu showing "admin" and "Password" with a text input field, an eye icon, and a question mark icon. At the bottom, there are two buttons: "OK" (blue) and "Cancel" (white).

3.1.3 Password Reset

You can reset the admin password by reserved email or security question.

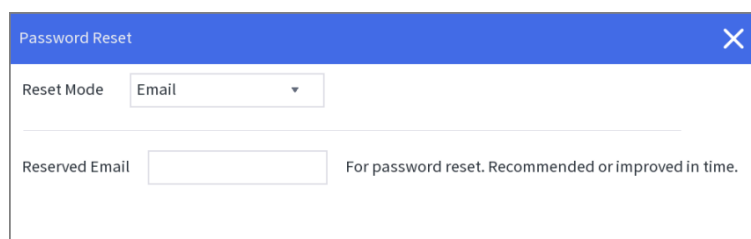
Reserved Email

1. Click  in the login page.
2. Select **Email** from the **Reset Mode** drop-down list, and then click **Next**.



If you did not configure the email address before, please enter the email address in this page.

Figure 3-5 Reset password through reserved email

A "Password Reset" dialog box with a blue header bar containing the text "Password Reset" and a close button (X). The main area is white and contains a "Reset Mode" dropdown menu with "Email" selected. Below this is a "Reserved Email" text input field. To the right of the input field, there is a note: "For password reset. Recommended or improved in time."

3. Follow the instructions on the device page to scan the QRcode, and then you will get the security code from the linked email address.
4. Enter the security code to reset the device.

Security Question

Answer the security questions to reset the password.

Figure 3-6 Reset password through security questions

The image shows a 'Password Reset' dialog box with a blue header and a close button (X) in the top right corner. Below the header, there is a 'Reset Mode' dropdown menu set to 'Security Question'. The dialog contains three sets of security questions, each with a question dropdown and an answer text input field. The questions are: 'Question 1: What is your favorite children's book?', 'Question 2: What was the first name of your first boss?', and 'Question 3: What is the name of your favorite fruit?'. At the bottom right, there are 'Next' and 'Cancel' buttons.

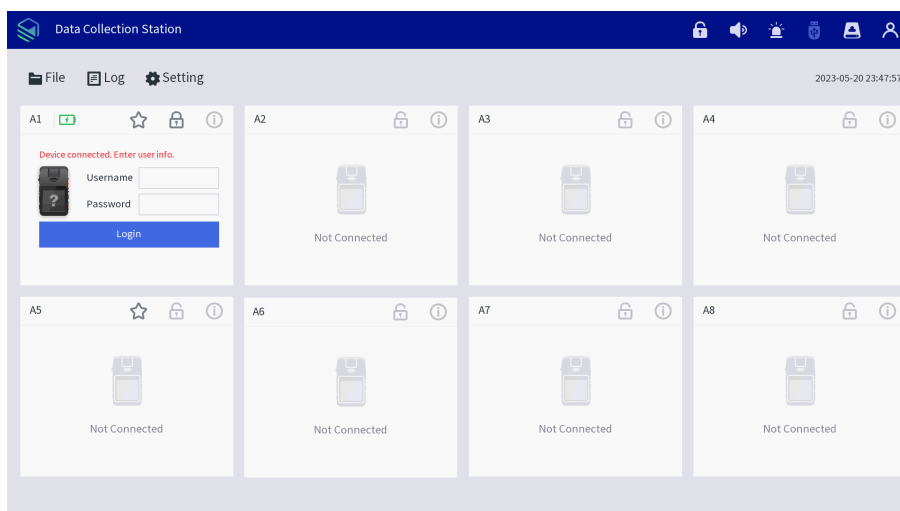
3.1.4 File Management

3.1.4.1 File Collection

If the body camera is connected with the enforcer, the Station will automatically collect data files from the connected body camera.

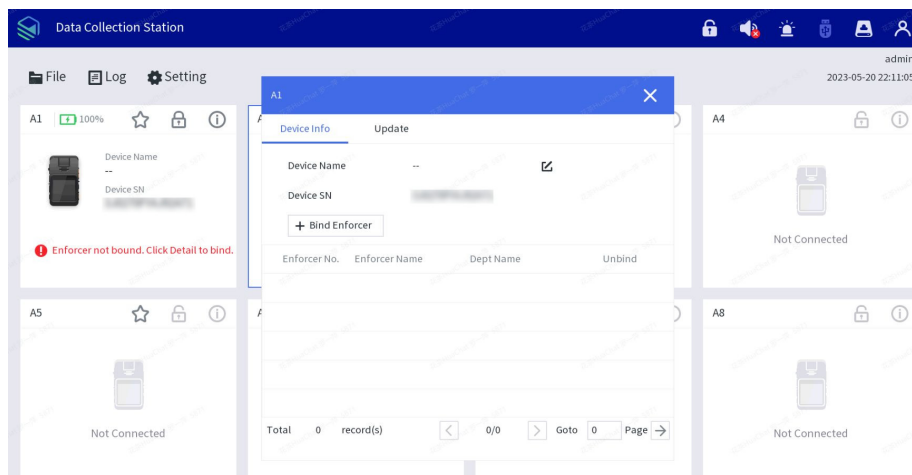
1. Connect the Station with the body camera.
2. Log in to the Station.
3. Enter the username and password, and then click **Login**.

Figure 3-7 Log in to the body camera



4. Click , and then click **Bind Enforcer** in the **Device Info** tab.

Figure 3-8 Bind enforcer



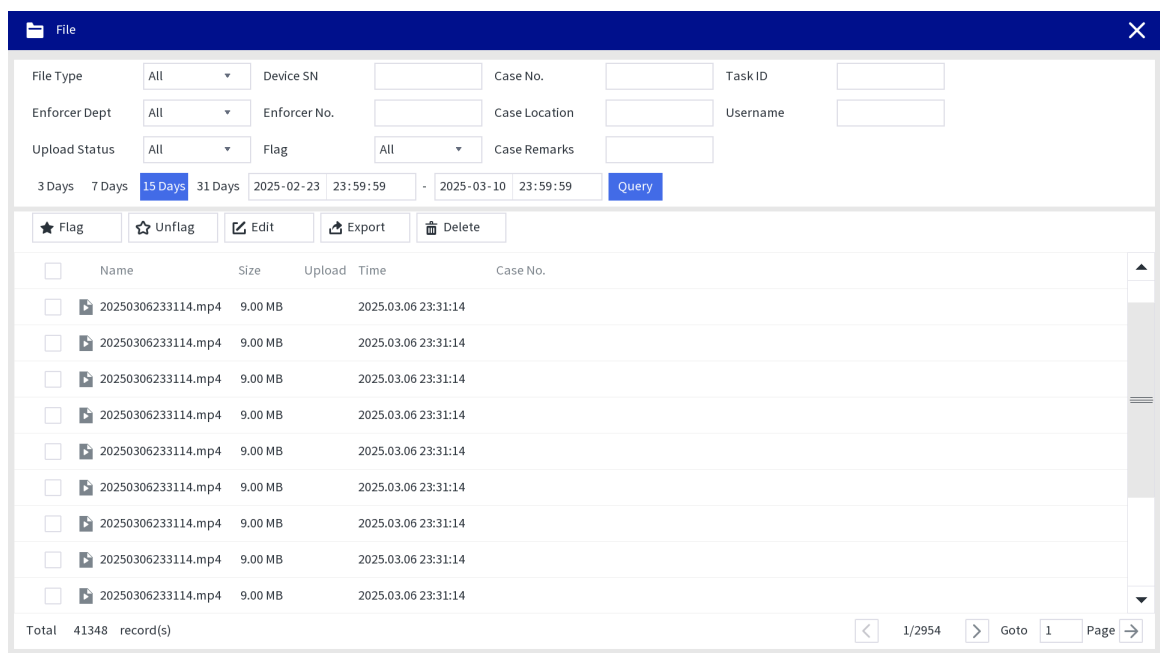
5. Select the enforcer, and then click **OK**.

3.1.4.2 Searching for Files

Procedure

- Step 1 Click **File** to check the information.
- Step 2 Configure the search conditions, and then click **Query**.
- Step 3 Double-click a file to view the details.

Figure 3-9 View files



3.1.4.3 Viewing Files

Double-click a file to open it.

3.1.5 Searching for Logs

You can view local logs, device logs, collection logs and upload logs.

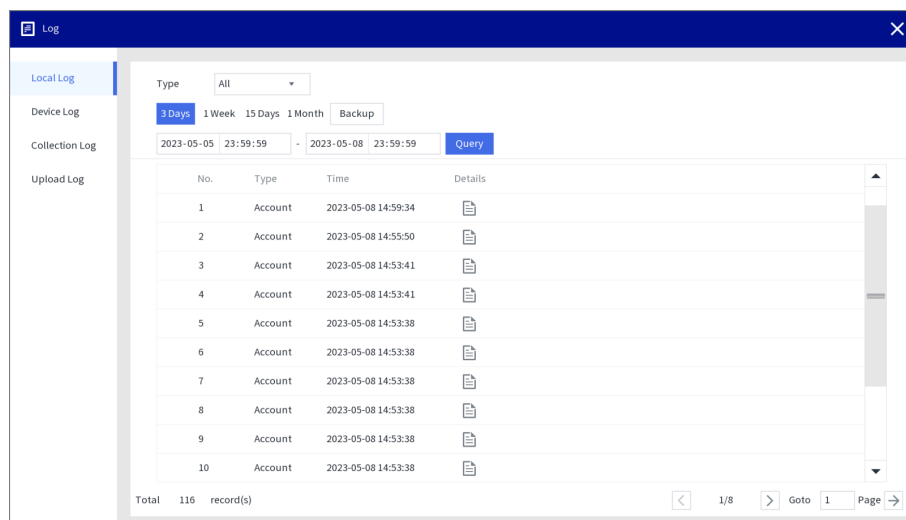
3.1.5.1 Local Log

Select **Log** > **Local log**, select the log type, enter the start time and end time, and then click **Query**.



- Click **Backup**, you can export the local log to the USB storage device.
- The maximum time range for log searching is 1 month.

Figure 3-10 Local log



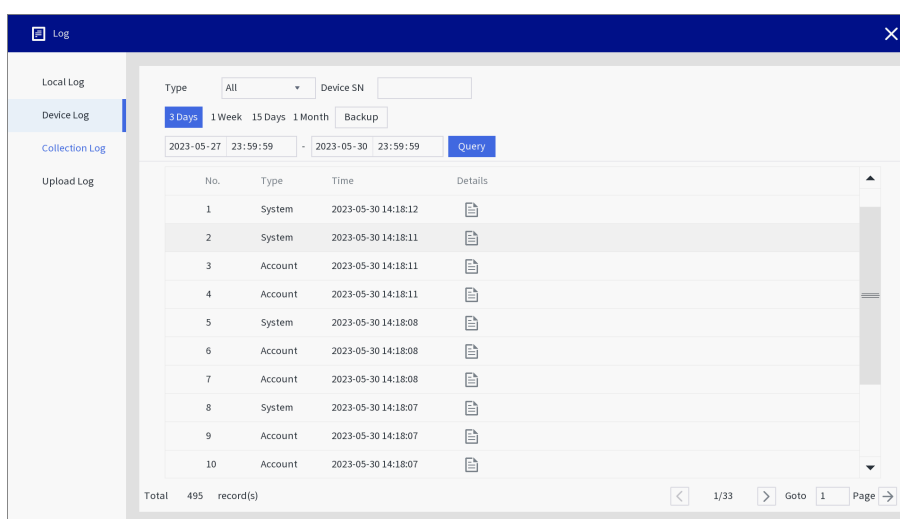
3.1.5.2 Device Log

Select **Log** > **Device Log**, select the log type, enter device SN, start time and end time, and then click **Query**.



- Click **Backup**, you can export the device log to the USB storage device.
- The maximum time range for log searching is 1 month.

Figure 3-11 Device Log



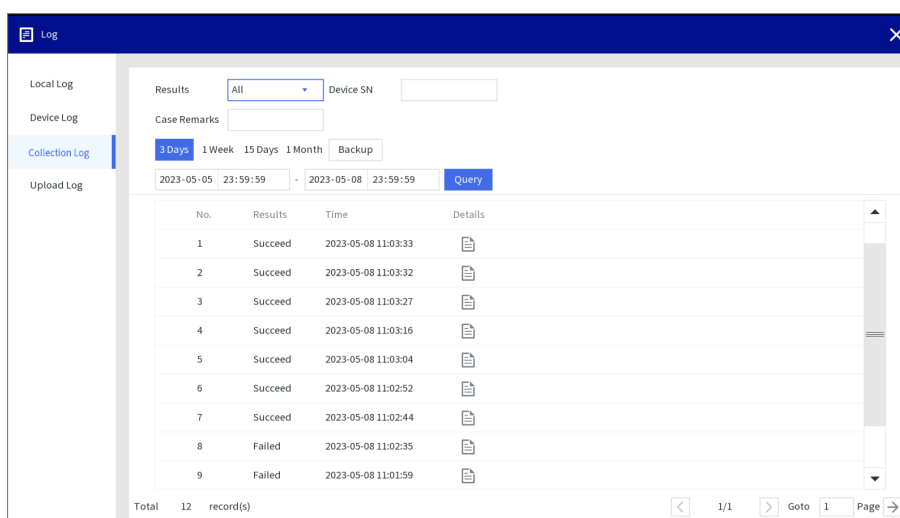
3.1.5.3 Collection Log

Select **Log** > **Collection Log**, select results, enter device SN, case remarks, start time and end time, and then click **Query**.



- Click **Backup**, you can export the collection log to the USB storage device.
- The maximum time range for log searching is 1 month.

Figure 3-12 Collection log



3.1.5.4 Upload Log

Select **Log** > **Upload log**, select the result, enter device SN, case No., case remarks, start time and end time, and then click **Query**.



- Click **Backup**, you can export the upload log to the USB storage device.
- The maximum time range for log searching is 1 month.

Figure 3-13 Upload log

3.1.6 Local Settings

3.1.6.1 User

Administrator can add user, delete user and edit user permissions.

3.1.6.1.1 User Management

Procedure

Step 1 Select **Setting** > **Account** > **User**.

Figure 3-14 User management

Step 2 Click **Add** to add users. All permissions are enabled by default.

Figure 3-15 Add users

Step 3 Click **OK**.

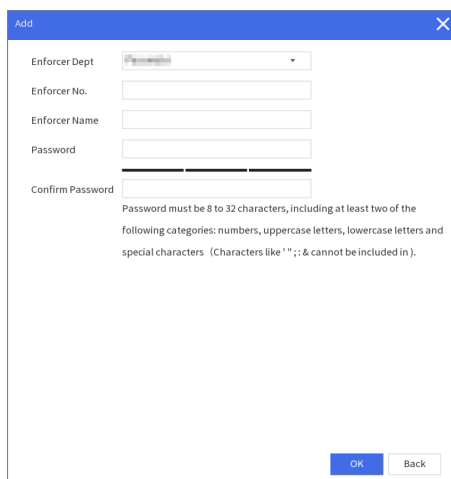
3.1.6.1.2 Enforcer Management

Select **Setting** > **Account** > **Enforcer**.

Adding Enforcer

Click **Add** to add users. Enter the related information, and then click **OK**.

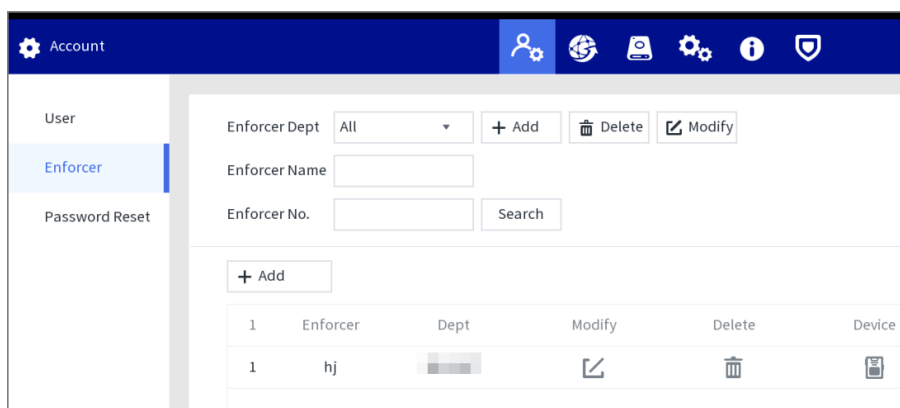
Figure 3-16 Add enforcer



Searching for Enforcer

You can search for enforcer through enforcer department, enforcer name, and enforcer No..

Figure 3-17 Search for enforcer



3.1.6.1.3 Resetting Password

Enable the function, and you can reset password by clicking  on the login page.

Procedure

- Step 1 Select **Setting** > **Account** > **Password Reset**, and then enable the password resetting function.



If the function is not enabled, you can only reset the password by resetting the Station.

Step 2 Enter the recovery email address and the security questions.

If you want to modify security question after successful setting, click **Reset** first.

Step 3 Click **Apply**.

Figure 3-18 Reset password

The screenshot shows a web interface for 'Account' management. On the left is a sidebar with 'User', 'Enforcer', and 'Password Reset' (selected). The main area is titled 'Password Reset' and contains an 'Enable' toggle switch (turned on), a 'Reserved Email' text input field, and a 'Security Question' section. Below the security question section, a note states: 'Admin password can be found after setting security questions.' There are three security questions, each with a dropdown menu and an 'Answer' text input field. The questions are: 'What is your favorite children's book?', 'What was the first name of your first boss?', and 'What is the name of your favorite fruit?'. At the bottom right of the form are 'Apply' and 'Back' buttons.

3.1.6.2 Network Management

3.1.6.2.1 TCP/IP

You can configure IP address, DNS (Domain Name System) server and other information according to network planning.



Make sure at least one Ethernet port has connected to the network before configuring IP address.

Procedure

Step 1 Select **Setting** > **Network** > **TCP/IP**.

Step 2 Configure the related information, and then click **Apply**.

Figure 3-19 TCP/IP

3.1.6.2.2 Port

Configure the port numbers and the maximum number of users (includes web and platform) that can connect to the device simultaneously.

Procedure

Step 1 Select **Setting** > **Network** > **Port**.

Step 2 Configure port parameters.

Figure 3-20 Configure port parameters

Table 3-2 Description of port parameters

Parameter	Description
Max Connection	Enter the max connection number. It ranges from 0 to 128.
TCP Port	Enter the number as needed. It is 37777 by default, and ranges from 1025 to 65535.
UDP Port	Enter the number as needed. It is 37778 by default, and ranges from 1025 to 65535.

Parameter	Description
HTTP Port	- Enter the number as needed. It is 80 by default, and ranges from 1 to 65535. - If the value you set is not 80, add the port number after the IP address when you are using browser to log in to the device.
HTTPS Port	Enter the number as needed. It is 443 by default, and ranges from 1 to 65535.
NTP Server Port	Enter the number as needed. It is 123 by default, and ranges from 1 to 65535.

Step 3 Click **Apply**.

3.1.6.2.3 Platform

Set up relevant functions for the interaction between the platform.

Register

Register the Station to a designated proxy server which acts as the transit to make it easier for the client software to access the Station.

Background Information

- The proxy server is deployed.
- The Station, the proxy server, and the device running the client software are on the same network.

Procedure

Step 1 Select **Setting > Network > Platform > Register**.

Step 2 Click  to enable the function, and then configure the parameters.

Figure 3-21 Register

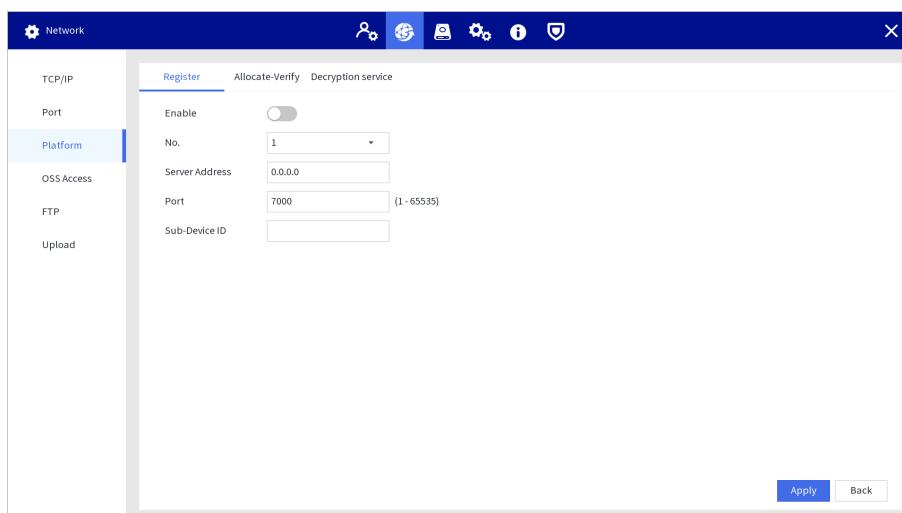


Table 3-3 Description of register parameters

Parameter	Description
Server Address	Enter the server IP address or the server domain that you want register to.

Parameter	Description
Port	Enter the port of the server.
Sub-Device ID	This ID is allocated by the server and used for the Station.

Step 3 Click **Apply**.

Allocate-Verify

Prerequisites

- The proxy server has been deployed, and the required law enforcement accounts have been registered on the server.
- The device, proxy server, and client terminals are on the same network.



The prerequisite is only for the platform user verification; there are no such restrictions for the auto allocating MPT.

Background Information

The allocation verification function allows the management of law enforcement accounts for devices to be handled centrally by the platform (proxy server). It also facilitates the automatic distribution of all connected body cameras by the devices themselves. The proxy server or collection station device serves as the centralized management system, reducing the configuration steps for customers and making it easier for them to use.

Procedure

Step 1 Select **Setting** > **Network** > **Platform** > **Allocate-Verify**.

Step 2 Configure the parameters.

Figure 3-22 Configure the allocate-verify function

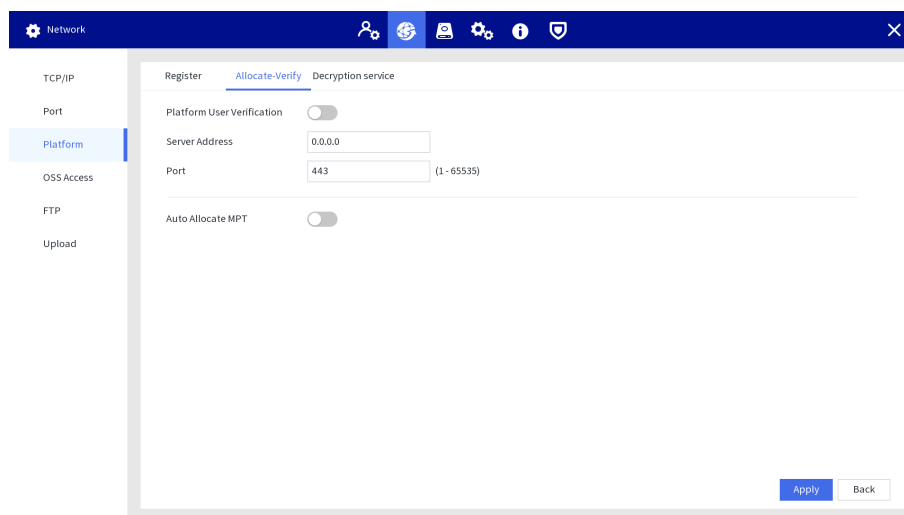


Table 3-4 Allocate-verify parameter description

Parameter	Description
Platform User Verification	Enable the function for unified verification of law enforcement users by the platform.
Server Address	The server IP address or server domain name for unified user verification.
Port	The port number of the server for unified user verification.

Parameter	Description
Auto Allocate MPT	Automatic allocation function of all MPTs by the collection station.



- Platform user verification and the auto allocate MPT function can be enabled separately.
- When auto allocate MPT function is enabled, two buttons will appear at the bottom of the main page. When the MPT is connected to the collection station, click **Put In** to get in the idle position; when disconnecting the MPT, click **Take Out**, and the collection station will automatically allocate the MPT based on the idle status, battery level, and priority of frequency.
- After enabling the platform user verification function, you need to enter the platform enforcement user for authentication when putting in and taking out the MPT.

Step 3 Click **Apply**.

Decryption Service

Prerequisites

- A proxy server has been deployed, with support for KMS key management functionality.
- The device, proxy server, and client terminals are all on the same network.

Background Information

Decryption Service allows devices to securely decrypt encrypted data files during playback by retrieving decryption keys from the proxy server. The server acts as a KMS (Key Management Service) to manage encryption keys, ensuring the security of customer data.



File encryption is performed on the MPT side. To successfully decrypt, the same decryption proxy server used by MPT is required.

Procedure

Step 1 Select **Setting > Network > Platform > Decryption service**.

Step 2 Click  to enable the function, and then configure the parameters.

Figure 3-23 Decryption service

The screenshot shows a web-based configuration interface for a network device. The top navigation bar includes a 'Network' section with icons for various settings. The left sidebar lists configuration categories: TCP/IP, Port, Platform (selected), OSS Access, FTP, and Upload. The main content area is titled 'Decryption service' and contains three tabs: 'Register', 'Allocate-Verify', and 'Decryption service'. The 'Decryption service' tab is active, displaying an 'Enable' toggle switch, a 'Server Address' input field, and a 'Port' input field with the value '443' and a range '(1 - 65535)'. At the bottom right of the configuration area are 'Apply' and 'Back' buttons.

Table 3-5 Description of decryption service parameters

Parameter	Description
Server Address	Enter the server IP address or the server domain that you want register to.
Port	Enter the port of the server.

3.1.6.2.4 OSS Access

Set the OSS access parameters to connect the device with the platform.

Procedure

- Step 1 Select **Setting** > **Network** > **Platform** > **OSS Access**.
- Step 2 Enable the function, and the configure the related parameters.

Figure 3-24 OSS access

Table 3-6 Description of OSS access

Parameter	Description
Server Address	Platform registered address.
Port	Platform registered port.
Username	Username and password to log in to the platform.
Password	
Device No.	Device No. should be the same as the parameter when the device is added to the platform.

Step 3 Enable the upload function, and then configure the parameters.

Table 3-7 Description of upload parameters

Parameter	Description
Port	It is 50000 by default.
Protocol	Supports HTTP and HTTPS . HTTPS is an encrypted transport protocol which could ensure the security of communication data and guard the user information.

Step 4 Click **Apply**.

3.1.6.2.5 FTP

Configure FTP server, and then you can save videos, audios and snapshots in the FTP server.

Prerequisites

Already deployed a FTP server, and created a user with the read & write permission.



The created FTP user should have write permission; otherwise the file uploading will fail.

Procedure

Step 1 Select **Setting** > **Network** > **FTP**.

Step 2 Enable FTP, select FTP type, and then configure the parameters.



You can select FTP or SFTP from the drop-down list. SFTP is recommended to enhance network security.

Figure 3-25 FTP setting

Table 3-8 Description of FTP parameters

Parameter	Description
Server Address	The IP address of the FTP/SFTP server.
Port	The port number of the FTP server. The default port is 22 for SFTP, and the default port is 21 for FTP.
Username	The username and password used to log in to the FTP server.
Password	
Storage Path	The destination path in the FTP server. Create the folder on FTP server. ● If you do not enter the name of remote directory, the system automatically creates the folders according to the IP and time. ● If you enter the name of remote directory, the system creates the folder with the entered name under the FTP root directory first, and then automatically creates the folders according to the IP and time.
Character Encode	Supports UTF-8 and GB2312. When messy codes are displayed on the server, switch the character encode.

Step 3 Click **Apply**.

3.1.6.2.6 Upload

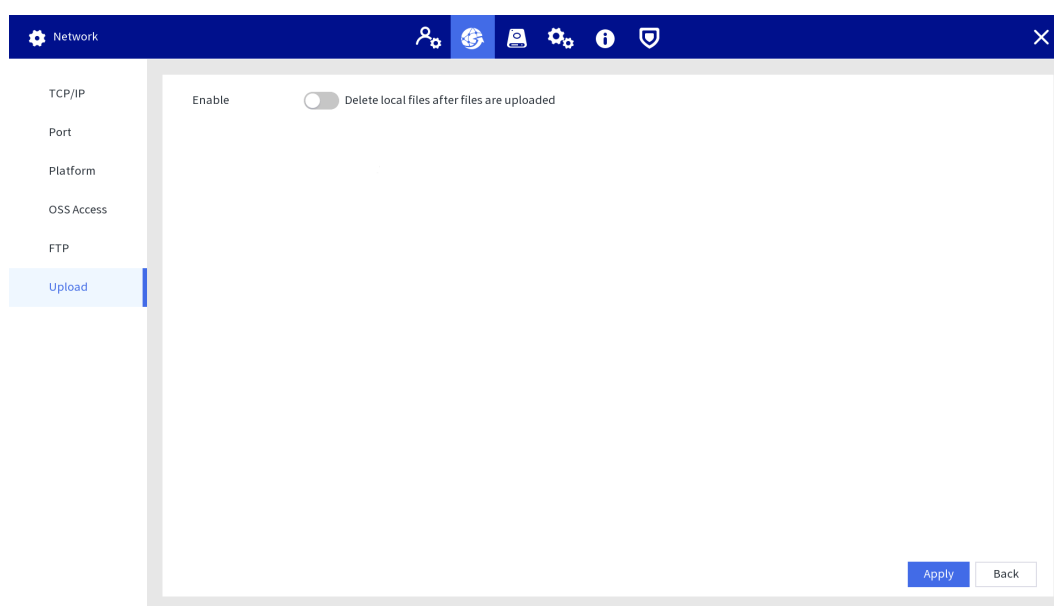
Enable this function, and then the local files will be deleted after the files are uploaded to the platform or FTP server.

Procedure

Step 1 Select **Setting** > **Network** > **Upload**.

Step 2 Click ☐ to enable this function.

Figure 3-26 Upload



Step 3 Click **Apply**.

3.1.6.3 Storage Management

You can manage the storage resources (such as recording files) and storage space to enhance storage space usage and data security.

3.1.6.3.1 Basic Configuration

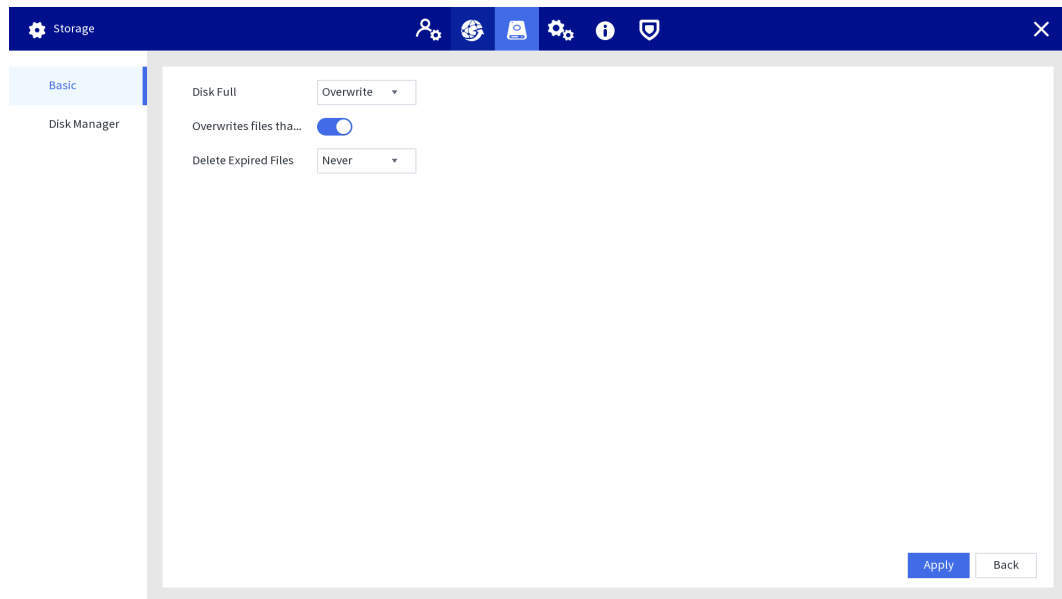
Procedure

Step 1 Select **Setting** > **Storage** > **Basic**.

Step 2 Configure the parameters.

- Disk full: Configure the settings for the situation that all the read/write disks are full, and there is no more free disk.
- Overwrites files that are not uploaded: If this function is disabled, files that are not uploaded will not be overwritten.
- Delete expired files: The default setting is **Never**, meaning historical files will not be deleted. When **Custom** is selected, you can configure the deletion of files that are 1 to 255 days. Once configured, the system will actively delete historical data that is older than the specified timeframe.

Figure 3-27 Basic configuration



Step 3 Click **Apply**.

3.1.6.3.2 Disk Manager

You can view disk information, format disk, and set the disk type according to the actual situation.

Procedure

Step 1 Select **Setting** > **Storage** > **Disk Manager**.

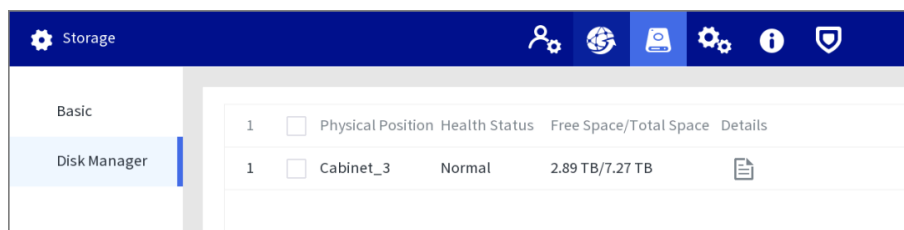
Step 2 Click  to view the details.

Step 3 (Optional) You can select an HDD, check **Format** to format the HDD.



This operation will delete all data in the HDD. Please be advised.

Figure 3-28 Disk Manager



3.1.6.4 System Management

3.1.6.4.1 Basic Configuration

You can set the logout time and decide whether to trigger alarm when network disconnection occurs.

Figure 3-29 Basic configuration

Table 3-9 Description of basic settings

Parameter	Description
Logout time	Set automatic logout interval. When you do not operate the Station within the set time, the Station will log out automatically. After auto logout, you need to log in again to operate. It ranges from 0–60 minutes, and 0 means the Station will not log out automatically.  To guarantee the safety of the Station account, we recommend you not to set the time as 0 minutes.
Offline	When Offline is enabled, an alarm is triggered when network disconnection occurs on any Ethernet port.
MPT Abnormally Disconnected Alarm	Enable the function to trigger an alarm in the event of abnormal disconnection of the MPT.

3.1.6.4.2 Date and Time

Procedure

Step 1 Select **Setting** > **System** > **Date&Time**.

Step 2 Configure the parameters.

You can set the time manually or through NTP.



In the same network, if the time of the body camera is not consistent with that of the Station, you may not view or play back videos.

Figure 3-30 Date and time

- Set the time manually

Set system time, format, and time zone according to the actual situation.

Table 3-10 Description of date and time parameters

Parameter	Description
System Time	Set the device system date and time. Click Sync PC to synchronize time with the PC from where you log in to the webpage.
Time Zone	Time zone of the current area.
Date Format	Select a date format from YYY MM DD , MM DD YYY , and DD MM YYY .
Date Separator	Select a separator between year, month, and date.
Time Format	Select a time format from 24-Hour and 12-Hour .
DST	When you enable DST (Daylight Saving Time), set DST type, start time and end time.  DST is a system to stipulate local time, in order to save energy. The DST is applied in some countries or regions. Enable or disable DST as needed.

- Set the time through NTP

Enable NTP, and then enter the server address or domain, port, and interval. After configuration, the system adjusts the device time according to the NTP server time.

Interval refers to the time interval that the device synchronizes time with the NTP server.

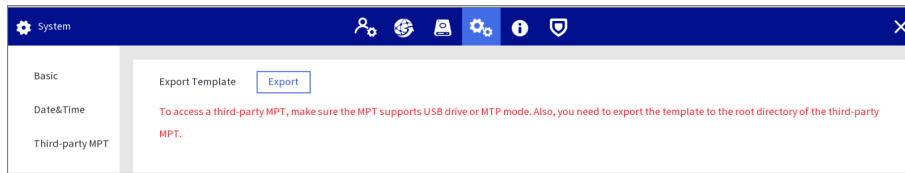
Step 3 Click **Apply**.

3.1.6.4.3 Third-party MPT

Select **Setting** > **System** > **Third-party MPT**.

Click **Export** to export the template.

Figure 3-31 Third-party MPT



3.1.6.5 Maintenance Center

3.1.6.5.1 System Info

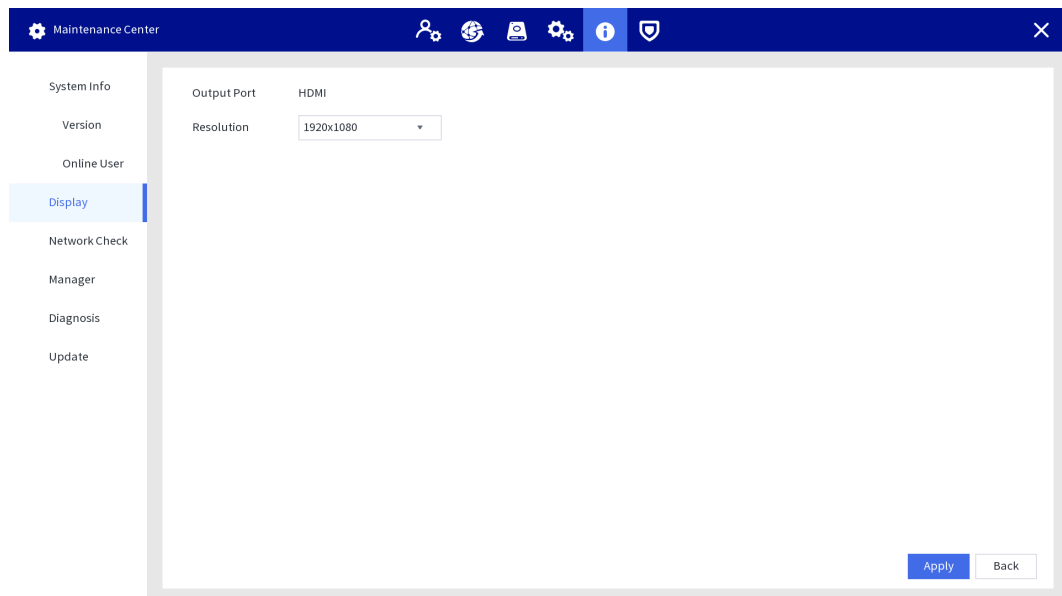
You can view the device information such as device model, hardware version, system version, and web version as well as the user information.

Select **Setting** > **Maintenance Center** > **System Info**.

3.1.6.5.2 Display

Select **Setting** > **Maintenance Center** > **Display** to check the output port and to set the resolution.

Figure 3-32 Display



3.1.6.5.3 Network Check

You can view the information of the user who is accessing the device, and the user list is updated in real time.

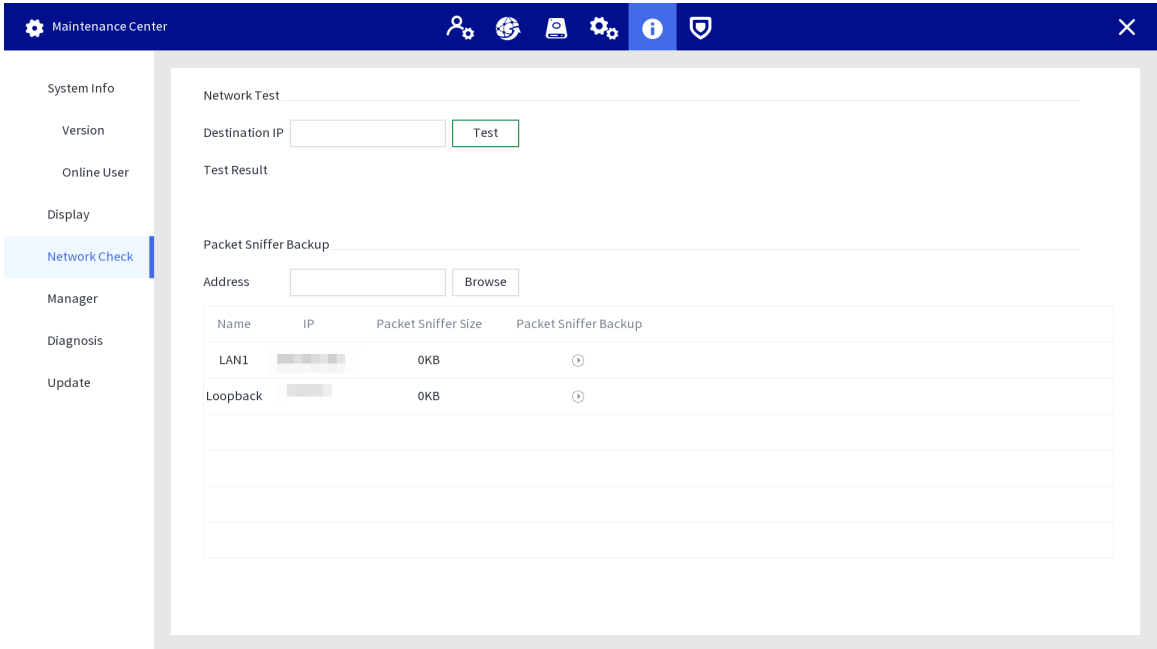
Procedure

Step 1 Select **Setting** > **Maintenance Center** > **Network Check**.



Click  to block a certain user for a period, and the blocking time can be set up to 65,535 seconds.

Figure 3-33 Network



The screenshot shows the 'Maintenance Center' interface. On the left is a sidebar with options: System Info, Version, Online User, Display, **Network Check** (highlighted), Manager, Diagnosis, and Update. The main area is titled 'Network Test' and contains a 'Destination IP' input field and a 'Test' button. Below this is a 'Test Result' section. Further down is the 'Packet Sniffer Backup' section, which includes an 'Address' input field and a 'Browse' button. At the bottom is a table with the following data:

Name	IP	Packet Sniffer Size	Packet Sniffer Backup
LAN1		0KB	
Loopback		0KB	

Step 2 In **Network Test**, set the destination IP, and then click **Test** to test the network.

Step 3 Click **Browse** in the **Packet Sniffer Backup** area to set the storage path of the captured package.

Step 4 Packet sniffer backup.

- Click  to enable the target filter as needed in the pop-up box, set the filtering address and port, and then click **OK**.



- ◇ After **Target Filter** is enabled, the system only captures the filtered address and IP.
- ◇ The captured package will be saved to the configured storage path, and the name is *Adapter-time*.

- Click  to stop capturing the package.

Figure 3-34 Target filter



The screenshot shows the 'Packet Capture' dialog box. It has a blue header with a close button (X). The 'Target Filter' toggle is turned on. Below it are two rows for address filtering:

Address Filtering 1: : (1 - 65535)

Address Filtering 2: : (1 - 65535)

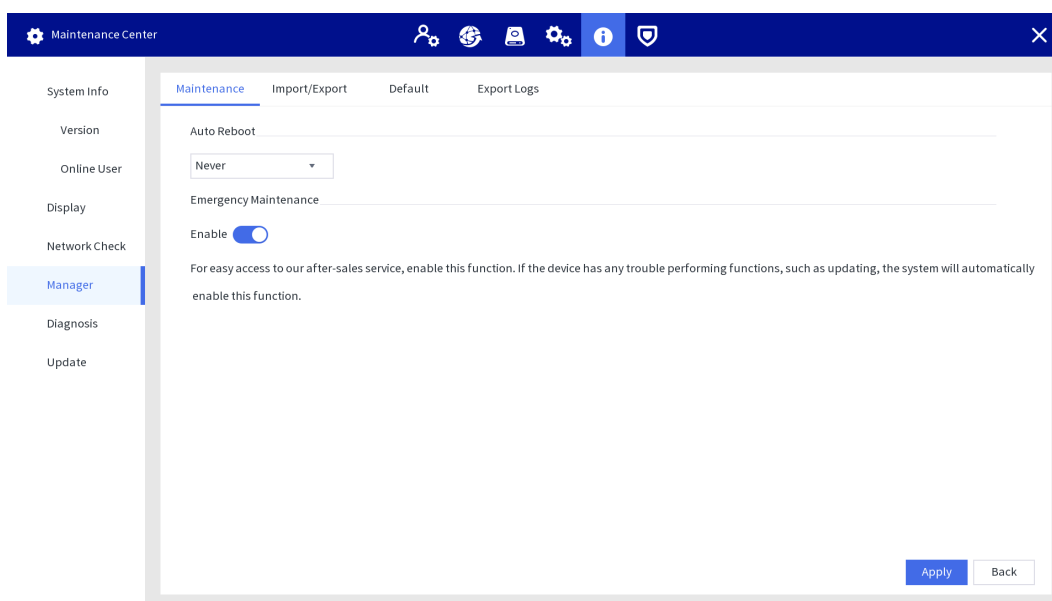
At the bottom right are 'OK' and 'Cancel' buttons.

3.1.6.5.4 Device Maintenance

Maintenance

1. Select **Setting** > **Maintenance Center** > **Manager** > **Maintenance**.
2. Configure the device maintenance as needed.
 - Auto reboot: Auto reboot the device as configured if the device runs for a long time.
 - Emergency maintenance: If the device runs an error or powered off during the upgrade, you can enable emergency maintenance to restart the device, clear configurations, and upgrade the device.

Figure 3-35 Device maintenance



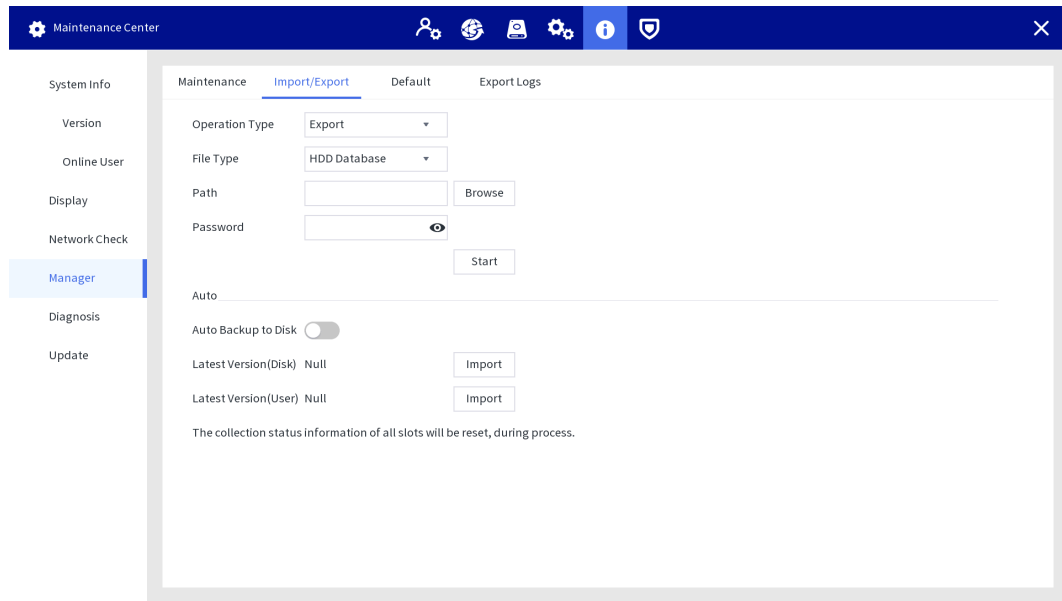
3. Click **Apply**.

Import/Export

Export the device data and user information for backup. When there is device exception, you can import the exported data to recover the data.

- Manual Device Maintenance:
 1. Select **Setting** > **Maintenance Center** > **Manager** > **Import/Export**.
 2. Select **Export** from the **Operation Type** list, select the file type and storage path, and then enter the password.
 3. Click **Start**.
 4. (Optional) When there is device exception, select **Import** from the **Operation Type** list, select the file type and storage path of the configuration file to be imported, and then enter the password.
 5. Click **Start**.
Import configuration file, and then restart the Station.

Figure 3-36 Import/Export



- Automatic Device Maintenance:

1. In the **Auto** area, enable **Auto Backup to Disk** according to your actual need.
2. Restore the disk database or user database.
 - ◇ When the latest version (hard disk) is displayed, click **Import** to restore the hard disk database file of the current displayed version.
 - ◇ When the latest version (user) is displayed, click **Import** to restore the hard disk database file of the current displayed version.



- ◇ Only configuration files exported from the Station of the same model are supported for import.
- ◇ During the automatic maintenance process, the data collection function will be toggled on and off, and the collection status information for all slots will be reset. Historical collection information (such as the number of completed collected files) will no longer be displayed.

Default

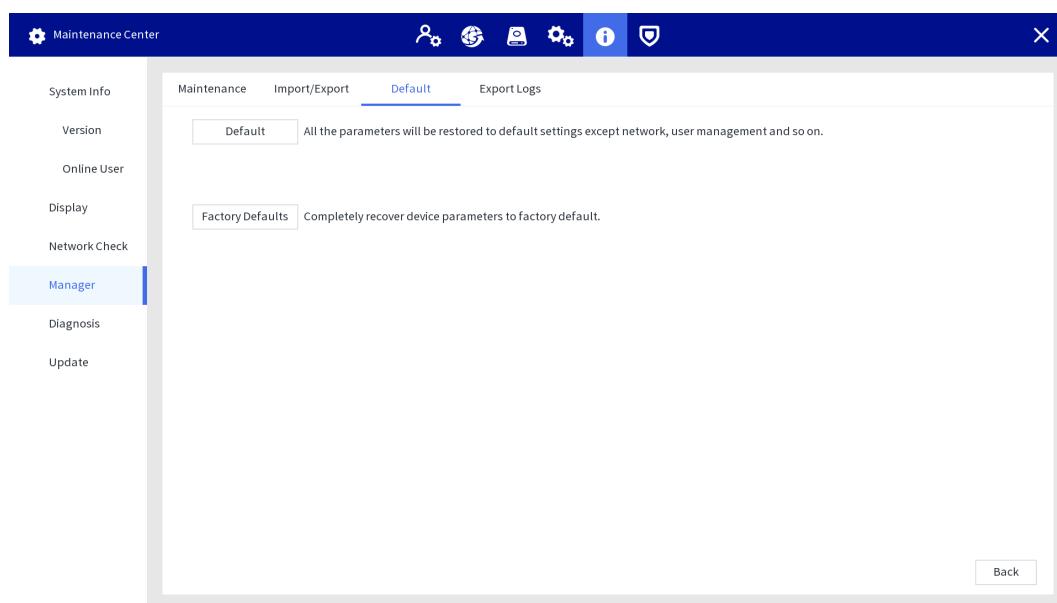
When the system runs slowly and has configuration errors, try to solve the problems by restoring the default settings.



Click **Factory Defaults**, all configurations except the data in the external storage will be deleted. You can delete data in an external storage by formatting the storage media and other methods.

1. Select **Setting > Maintenance Center > Manager > Default**.
2. Click **Default** or **Factory Defaults**.

Figure 3-37 Default



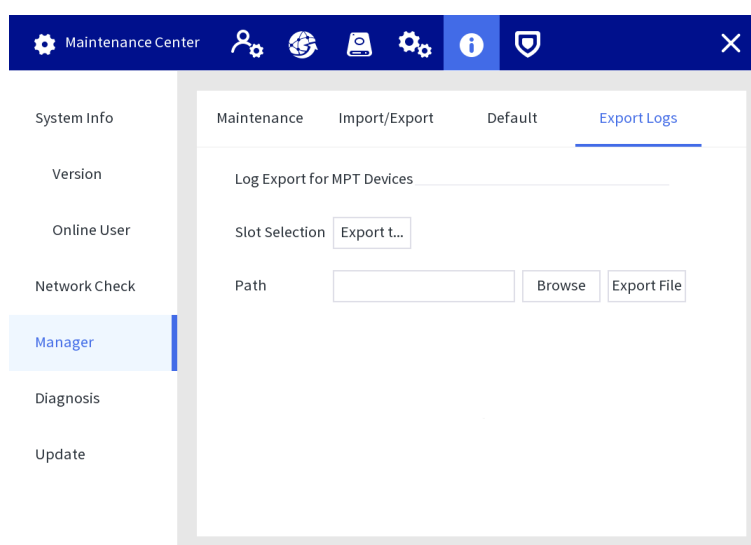
- Default: Tap **Default**, and the parameters such as except network, user management will be restored to default setting.
- Factory default: Tap **Factory Defaults**, and the tip dialog is displayed. Tap **OK**. All parameters will be restored to the factory default settings.

Export Logs

Export the operation logs of the body camera for troubleshooting and analysis. Connect an external USB storage device and export the operation logs to the specified path on the storage device.

1. Select **Setting** > **Maintenance Center** > **Manager** > **Export Logs**.
2. Click **Export to Disk** to select the slot.

Figure 3-38 Export logs

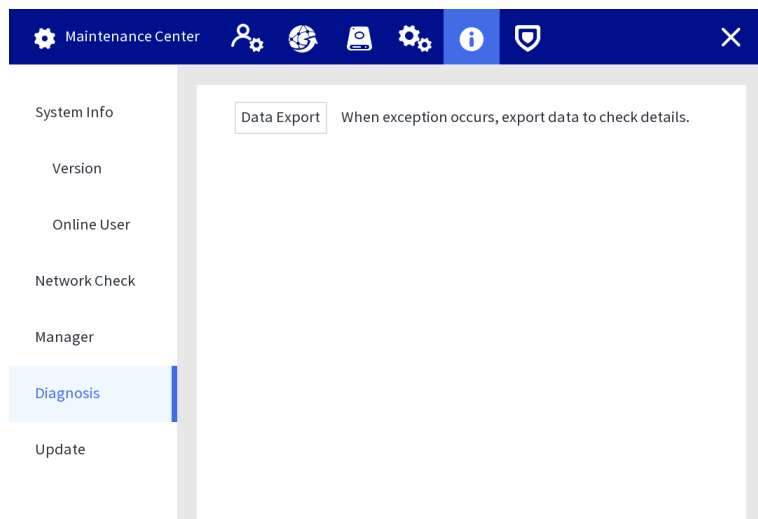


3. Click **Browse**, and then select the MPT and the path.
4. Click **Export File**.

3.1.6.5.5 Diagnosis

Select **Settings** > **Maintenance Center** > **Diagnosis** > **Data Export** to export data of the device health, such as emmc lifespan for issue verification.

Figure 3-39 Diagnosis

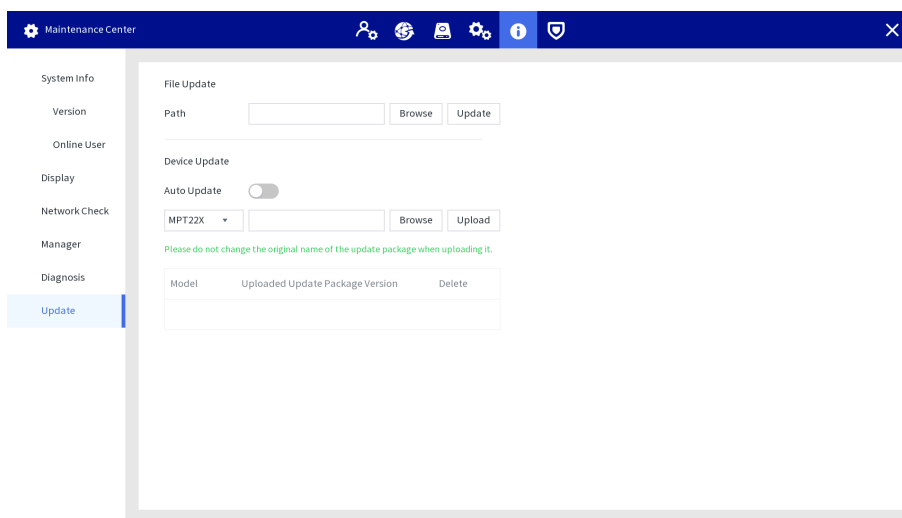


3.1.6.5.6 Update

System Update

- File Update: Insert a USB flash drive with update file in bin format, and then import the update file to the Station to update the system version.
 1. Select **Setting** > **Maintenance Center** > **Update**.
 2. Select the update file, and then click **Update**.

Figure 3-40 Update



- Device Update: Before updating, upload the update files to the Station according to the types of body cameras.
 - ◇ Auto update

Enable the auto update function. The body camera will detect the update files and update automatically after accessing the Station.

◇ Manual update

When the auto update function is disabled, select the update file, and then tap **Upload** to

upload the file of latest version. Tap ⓘ on the home screen, and then tap the **Update** tab to update the device.

3.1.6.6 Security

3.1.6.6.1 Security Status

Detect the user and service, and scan the security modules to check the security status of the Station. When abnormality appears, you can process it timely.

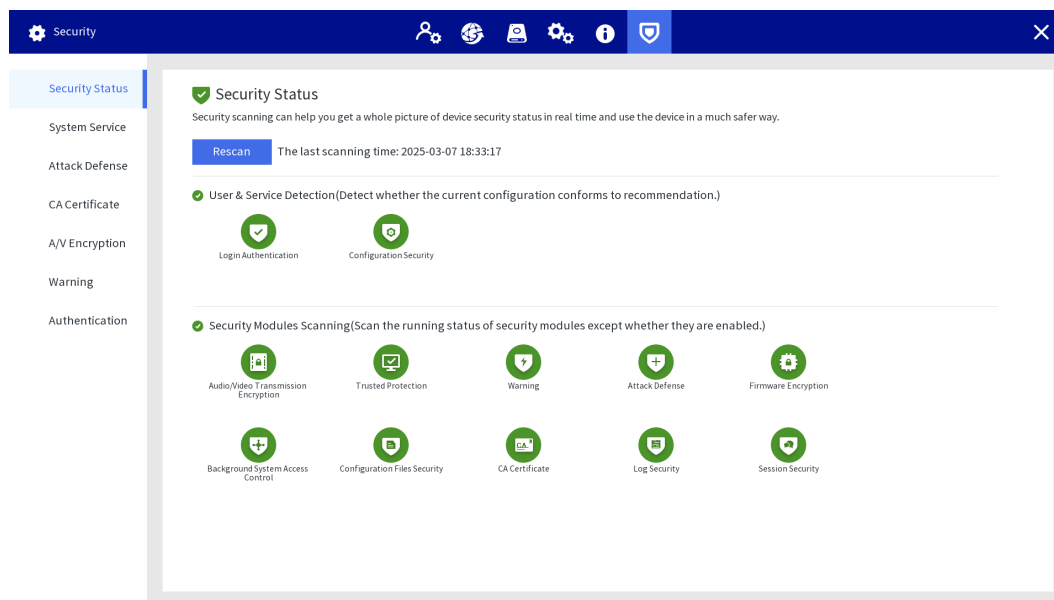
- User and service detection: Detect login authentication, user status, and configuration security to check whether the current configuration conforms to recommendation.
- Security modules scanning: Scan the running status of security modules, such as audio/video transmission, trusted protection, securing warning and attack defense, not detect when they are enabled.

Procedure

Step 1 Select **Setting** > **Security** > **Security Status**.

Step 2 Click **Rescan** to scan the security status of the Station.

Figure 3-41 Security status



Results

After scanning, different results will be displayed with different colors. Yellow indicates that the security modules are abnormal, and green indicates that the security modules are normal.

Click **Details** to view the details of the scanning result.

- Ignore: Ignore the exception, and this part will not be scanned in next scanning.



Click **Rejoin Detection**, the exception will be scanned in next scanning again.

- Optimize: The corresponding screen is displayed, and then you can edit the configuration to clear the exception.

3.1.6.6.2 System Service

Select **Setting** > **Security** > **System Service**.

Basic Services

Configure the basic services parameters, and then click **Apply**.

Figure 3-42 Basic services

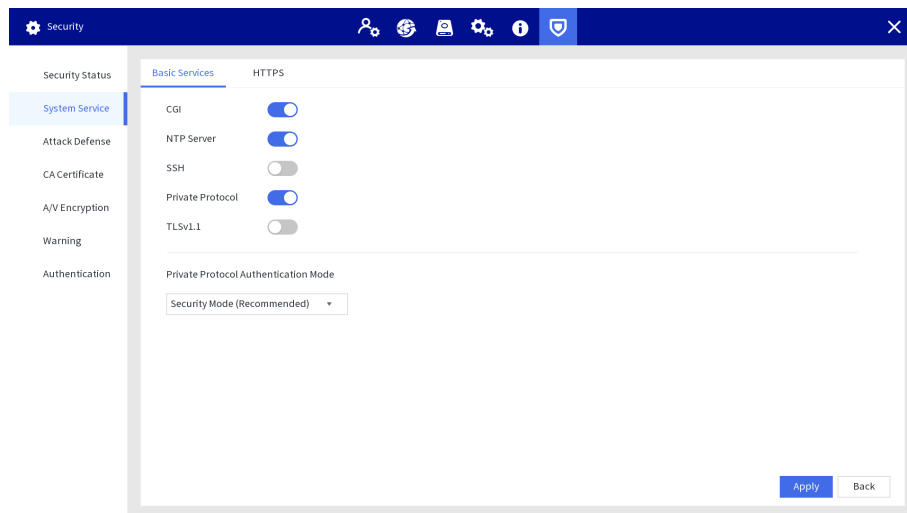


Table 3-11 Description of basic service parameters

Parameter	Description
CGI	Enable this function, and then devices can access the Station through this service. It is enabled by default.
NTP Server	After enabling this function, the Station is used as a NTP server, which can be used to synchronize the time of the body camera. It is enabled by default.
SSH	You can enable SSH authentication to realize safety management.
Private Protocol	After enabled, you can set the private protocol authentication mode.
TLSv1.1	Encryption Protocol.
Private Protocol Authentication Mode	Select private protocol authentication mode to guarantee the device security when login.

HTTPS

After enabled this function, the computer can log in to the device by HTTPS to ensure the security of communication data and the user information.

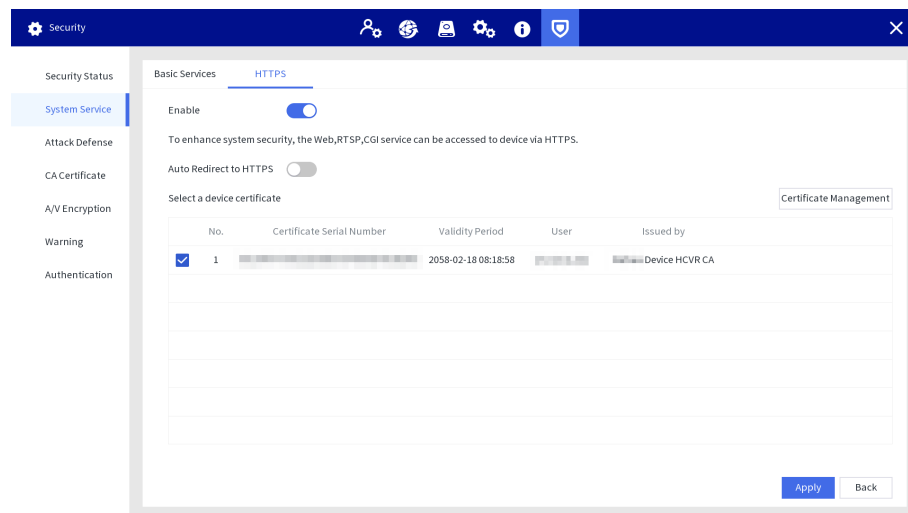


We recommend you to enable HTTPS service. If the service is disabled, there might be risk of data leakage.

1. Click ☐ to enable this function.
2. Select the certificate.

If there is no certificate in the list, click **Certificate Management** to import a certificate.

Figure 3-43 HTTPS



3. Click **Apply**.



Auto Redirect to HTTPS is disabled by default. When you enable the HTTPS service, you can access the device using either the HTTPS or HTTP protocol. Once **Auto Redirect to HTTPS** is enabled, accessing the device via HTTP will automatically switch to the HTTPS protocol, so you cannot use the HTTP protocol anymore.

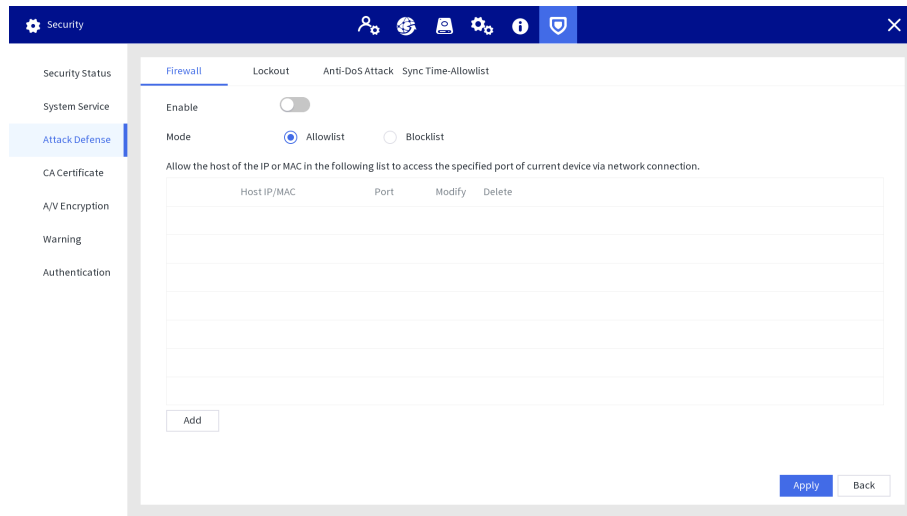
3.1.6.6.3 Attack Defense

Select **Setting** > **Security** > **Attack Defense**.

Firewall

1. Click ☐ to enable this function.

Figure 3-44 Firewall



2. Select the access mode.

Allowlist and blocklist cannot be enabled at the same time.

- Allowlist: Only the IP/MAC in the allowlist can access the Station.
- Blocklist: The IP/MAC in the blocklist cannot access the Station.

3. Click **Add** to add the host IP/MAC address into allowlist or blocklist, and then click **OK**.

Figure 3-45 Add allowlist/blocklist

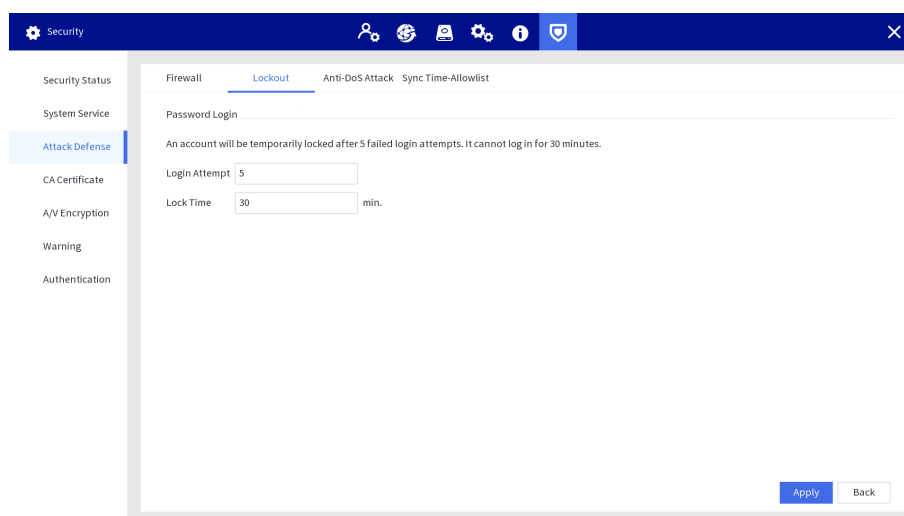
4. Click **Apply**.

Logout

You can set the number of allowed login attempts and lock time for password login. If the number of failed login attempts reaches the defined threshold, the account will be temporarily locked.

- Login attempt: Upper limit of login attempts. If the number of failed login attempts reaches the defined threshold, the account will be locked.
- Lock time: The period during which you cannot log in after the number of failed login attempts reaches upper limit.

Figure 3-46 Logout

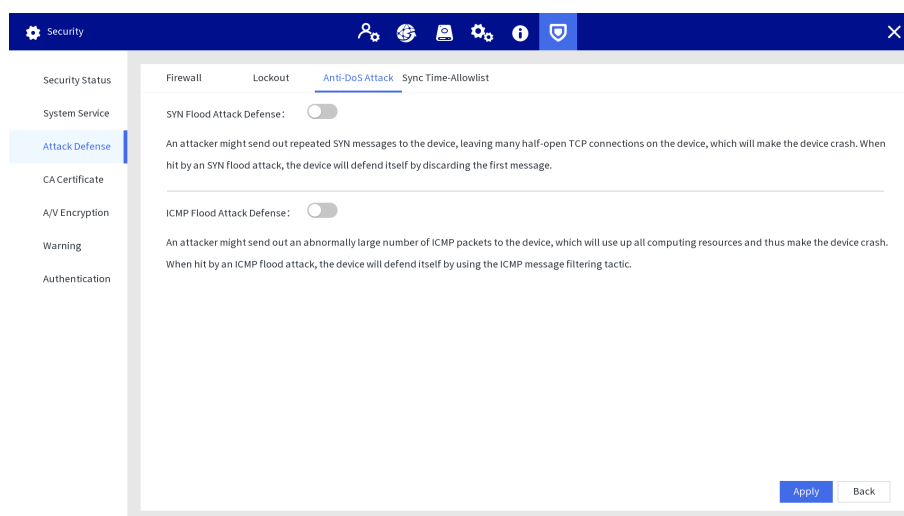


Anti-DoS Attack

Set the attack defense mode to defend the device against Dos (Denial of Service) attack.

Enable **SYN Flood Attack Defense** or **ICMP Flood Attack Defense** as needed, and then click **Apply**.

Figure 3-47 Anti-DoS attack

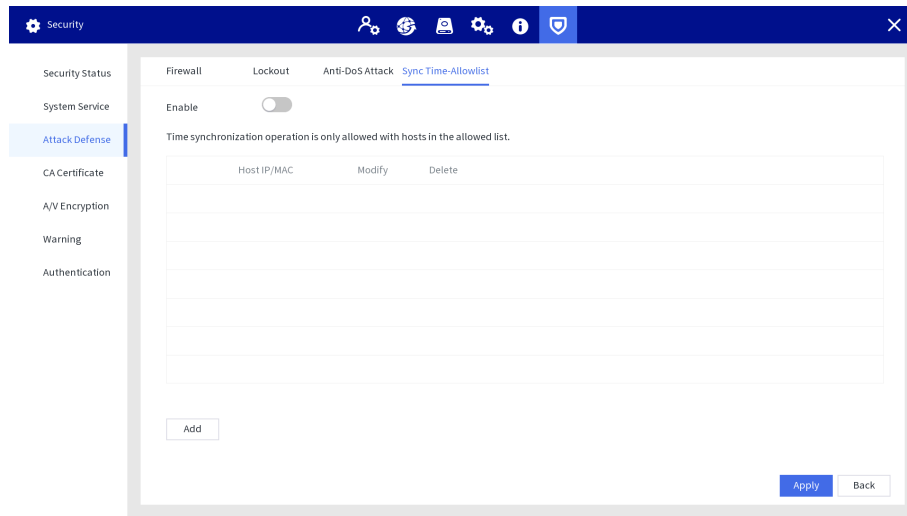


Sync Time-Allowlist

Set the IP address of hosts that are allowed to sync and change system time, in case that multiple hosts calibrate the system time with the Station several times.

1. Click ☐ to enable the function.

Figure 3-48 Sync Time-Allowlist



2. Click **Add** to add the IP/MAC of the source host through IP address or IP segment.
3. Click **Apply**.

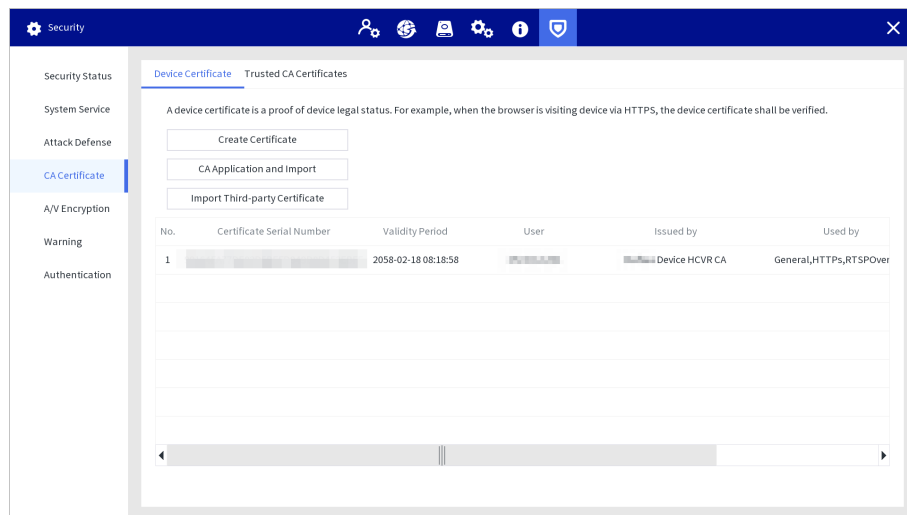
3.1.6.6.4 CA Certificate

Create a certificate or upload an authenticated certificate, and then you can log in through HTTPS with web browser.

Procedure

- Step 1 Select **Setting** > **Security** > **CA Certificate** > **Device Certificate**.

Figure 3-49 Device certificate



- Step 2 Manage the certificate.

- Create certificate
 - Enter the certificate information, and then click **Create**.
 - After the certificate is created successfully, you can view the created certificate on the **Device Certificate** page.
- CA application and import
 1. Enter the certificate information, and then click **Create** to save the certificate to an external device

2. Apply for the CA certificate from the third-party certificate authority.
3. Import the CA certificate.
 - a. Save the CA certificate to a USB flash drive, and then insert the drive to the Station.
 - b. Click **Import Certificate** on the **CA Application and Import** page.
 - c. Import the certificate according to the instruction.

After the certificate is imported successfully, you can view the created certificate on the **Device Certificate** page.

Figure 3-50 CA application and import

- Import third-party certificate

Select the certificate and private key file, enter the private key password, and then click **Import**.

Step 3 Select **Trusted CA Certificates** tab, and then click **Install Trusted Certificate**.

CA certificate is a digital certificate for the legal identity of the Station. For example, when the Station accesses the LAN through 802.1x, the CA certificate is required.

Step 4 Click **Browse** to select the certificate on the pop-up box, and then click **Import**.

After the certificate is imported successfully, you can view the created certificate on the **Device Certificate** page.

Related Operations

- : Download the certificate.
- : Delete the certificate.

3.1.6.6.5 A/V Encryption

Supports audio and video encryption during data transmission.

Background Information



We recommended you to enable A/V Encryption function. There might be safety risk if this function is disabled.

Procedure

- Step 1 Select **Setting** > **Security** > **A/V Encryption**.
- Step 2 Configure the parameters.

Figure 3-51 A/V encryption

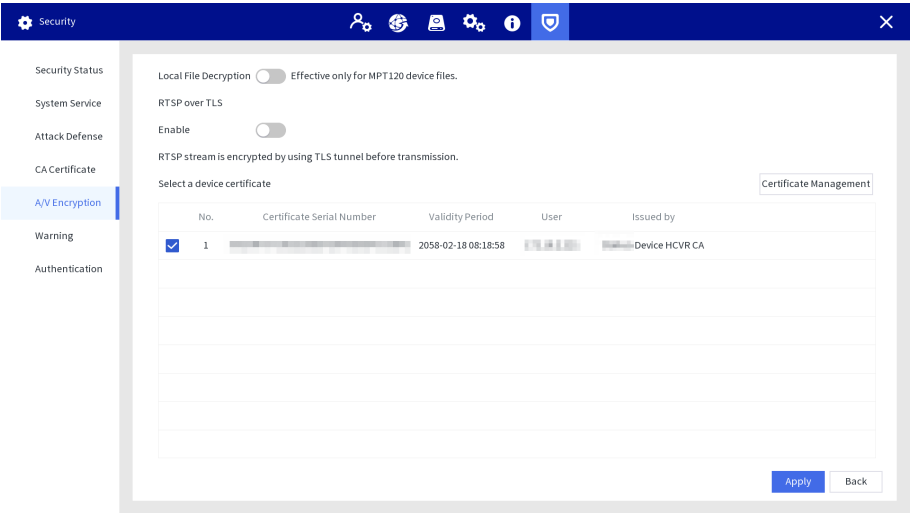


Table 3-12 Description of A/V description

Encryption Type	Parameter	Description
Local File Decryption	Enable	When you collect encrypted files from the MPT120 devices, the Station performs decryption before collection.
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS. Click next to Enable , and then select certificate in the Select a device certificate list. There might be safety risk if RTSP over TLS is disabled.
	Certificate Management	The created or imported certificate will be displayed in the Select a device certificate list, and then select certificate.

- Step 3 Click **Apply**.

3.1.6.6.6 Security Warning

Security Warning

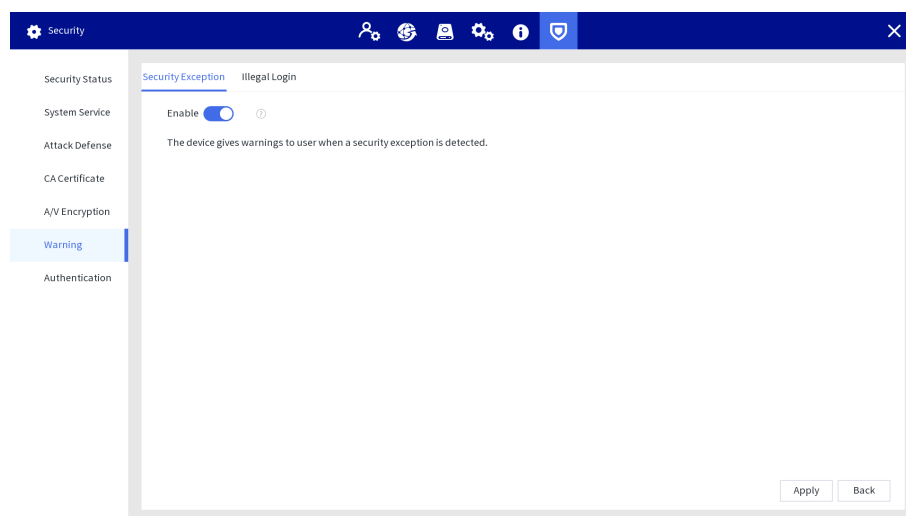
1. Select **Setting** > **Security** > **Warning** > **Security Exception**.
2. Click ☐ to enable the function.



Click to view the details of the security exception event.

3. Click **Apply**.

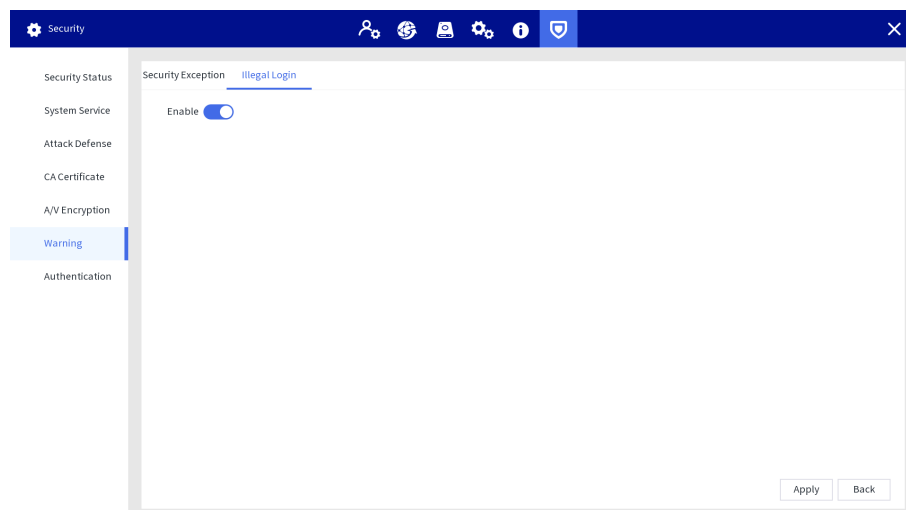
Figure 3-52 Security exception



Illegal Login

1. **Setting** > **Security** > **Warning** > **Illegal Login**.
2. Click ☐ to enable the function.
3. Click **Apply**.

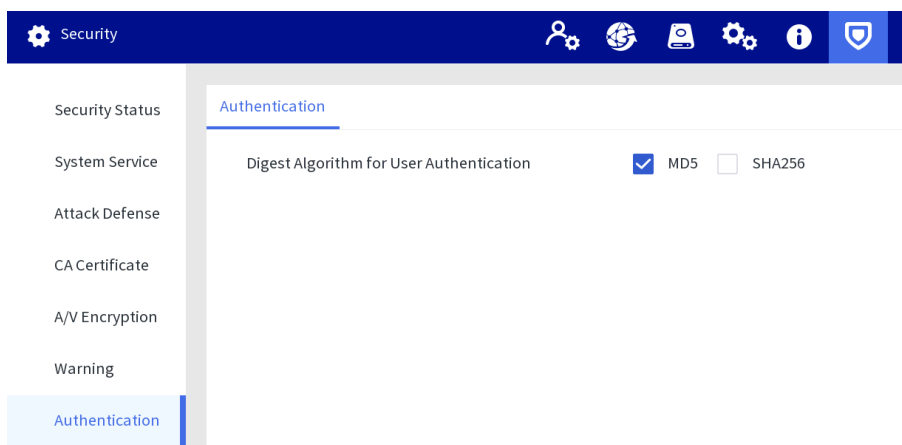
Figure 3-53 Illegal login



3.1.6.6.7 Security Authentication

Set up the security authentication method, supporting MD5 and SHA256, to enhance the security of user authentication and data protection.

Figure 3-54 Select digest algorithm for user authentication



3.1.6.7 Platform Configuration

After adding the Station to the platform, you can remotely configure the Station, add devices, and perform other operations on the platform.

Background Information

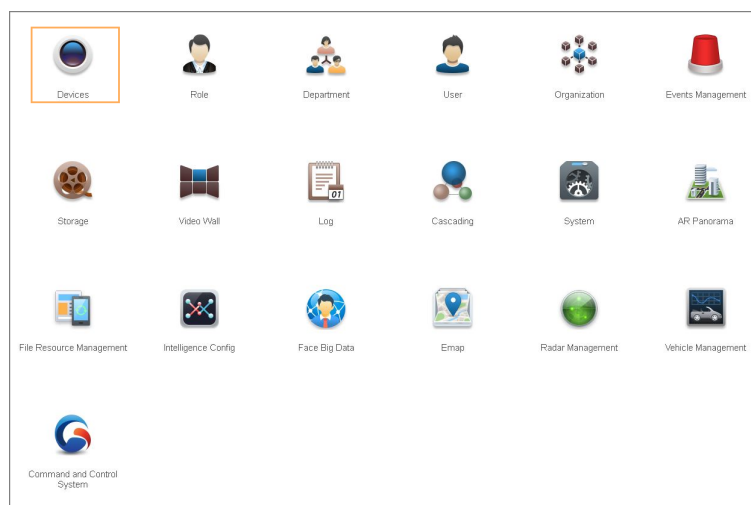


The following operations are for reference only. The actual operation might vary depending on the actual platform you are using.

Procedure

Step 1 Log in to the platform, and then on the home page, click **Devices**.

Figure 3-55 Home page



Step 2 Click **Add**, and then configure the parameters.

Figure 3-56 Login information

The screenshot shows a web-based 'Add Devices' dialog box. At the top, there are two tabs: '1. Login Info' (active) and '2. Device Info'. The 'Login Info' tab contains the following fields:

- Protocol: A dropdown menu.
- Manufacturer: A dropdown menu.
- Add Type: A dropdown menu with 'IP Address' selected.
- Device Category: A dropdown menu with 'Encoder' selected.
- IP Address: A text input field.
- Device Port: A spinner control with '37777' selected.
- User: A text input field with 'admin' entered.
- Password: A password input field with asterisks.
- Organization Code: A dropdown menu with 'root' selected.
- Domain Name: A dropdown menu with 'defaultPaaS' selected.
- Device Access Gateway: An unchecked checkbox.

At the bottom right, there are 'Add' and 'Cancel' buttons.

Table 3-13 Parameters of adding device

Parameter	Description
Add Type	Two methods are available. ● Auto Registration: The most common method to add devices to the platform. ● IP Address: Use the IP address of the Station to add it to the platform.
Device Category	Select Encoder .
IP Address	When the Add Type is IP Address , enter the IP address and port of the Station. By default, the port number is 37777.
Device Port	
User	Enter the username and password used to log in to the Station.
Password	
Organization Code	Select the organization that the Station belongs to. The default organization is root.
Domain Name	Select a domain name. The default domain name is default PaaS .

Step 3 Click **Add**, and then configure the device information.

Figure 3-57 Device information

The screenshot shows a web-based configuration window titled "Add Devices". It has two tabs: "1. Login Info" and "2. Device Info", with the second tab being active. The "2. Device Info" section contains four input fields: "Device Name" with the value "caijizhan", "Type" set to "Collection Station", "Video Channel" set to "1", and "Alarm Input Channel" set to "0". At the bottom of the window are three buttons: "Previous", "Continue Add", and "OK".

Table 3-14 Device information parameters

Parameter	Description
Device Name	Create a name to identify the Station on the platform.
Type	Select Collection Station .
Video Channel	Select a video channel for the Station. The default channel is 1.
Alarm Input Channel	Select an alarm input channel for the Station. The default channel is 0.

Step 4 (Optional) Click **Continue Add** to add more Stations.

Step 5 Click **OK**.

3.2 Web Configuration

3.2.1 Device Initialization

When starting the device for the first time, you need to configure the login password of the admin user.

Background Information



For account security, we recommend you keep the password properly and change it regularly.

Procedure

Step 1 Open the browser, enter the IP address (the default IP address is 192.168.1.108) of the device in the address bar, and then press the Enter key.

- Step 2 Select the region and language, and then click **Next**.
- Step 3 Read the end-user license agreement and privacy policy, select **I have read and agree to all terms**, and then click **Next**.
- Step 4 Set the time and time zone, and then click **Next**.
- Step 5 Configure and confirm the password, and then click **Next**.

Figure 3-58 Password Setting

Username: admin

Password

Confirm Password

Next

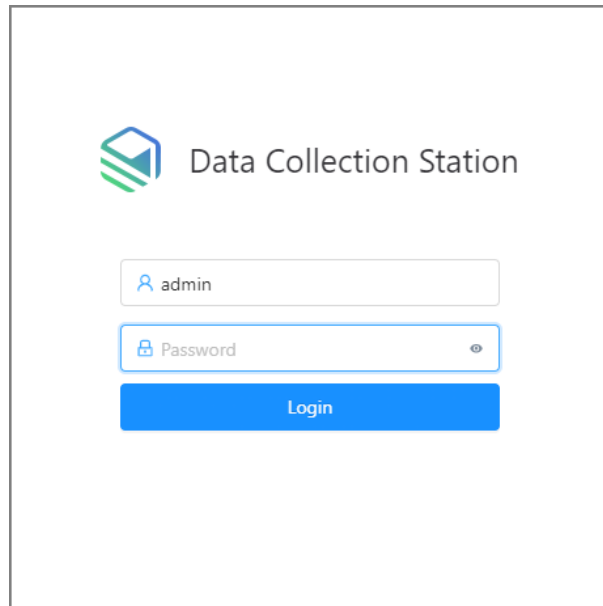
- Step 6 (Optional) Set security questions.
You can reset the admin password by reserved email or security question. For details, see "3.1.3 Password Reset".
- Step 7 Click **Next**.
The initialization is finished.

3.2.2 Login

Procedure

- Step 1 Enter the IP address of the Station in the address bar of the IE browser, and then press the Enter key. For details, see "3.1.6.2.1 TCP/IP".

Figure 3-59 Login



The login interface for the Data Collection Station. It features a logo on the left and the text "Data Collection Station" on the right. Below this, there are two input fields: the first is labeled "admin" with a user icon, and the second is labeled "Password" with a lock icon and a toggle eye icon. A blue "Login" button is positioned below the password field.

Step 2 Enter the username and password.

- The administrator account is **admin** by default.
- The password is the one set in "3.2.1 Device Initialization".

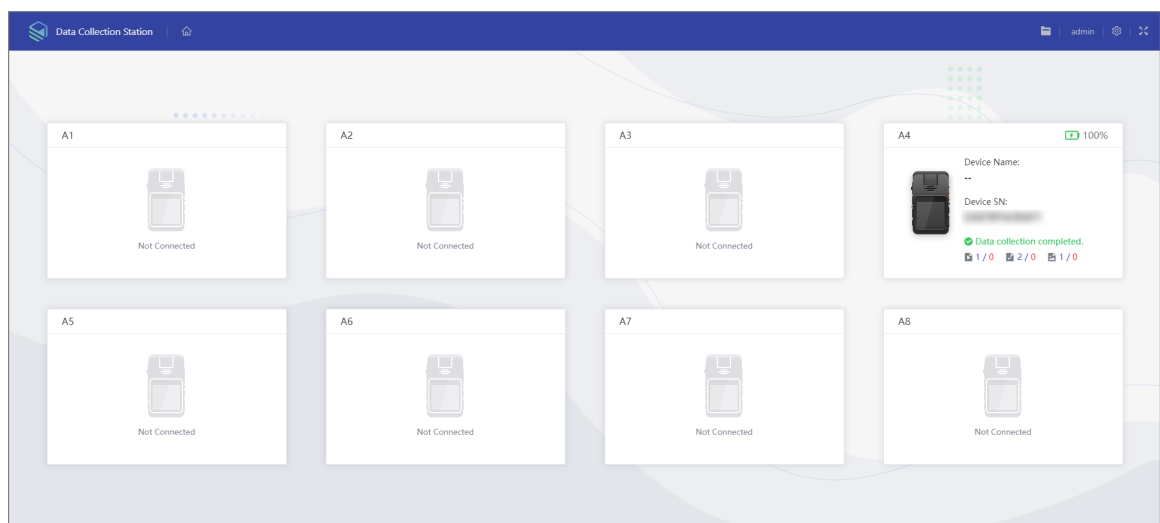
Step 3 Click **Login**.

3.2.3 File Management

3.2.3.1 Collecting Files

The Station collects data files from the body camera. Before the Station automatically collects data, it is necessary to log in to the body camera and bind the enforcer on this device. For details, see "3.1.4.1 File Collection".

Figure 3-60 Upload files



3.2.3.2 Searching for Files

Search for files collected from the Station, including videos, sound recording, and images.

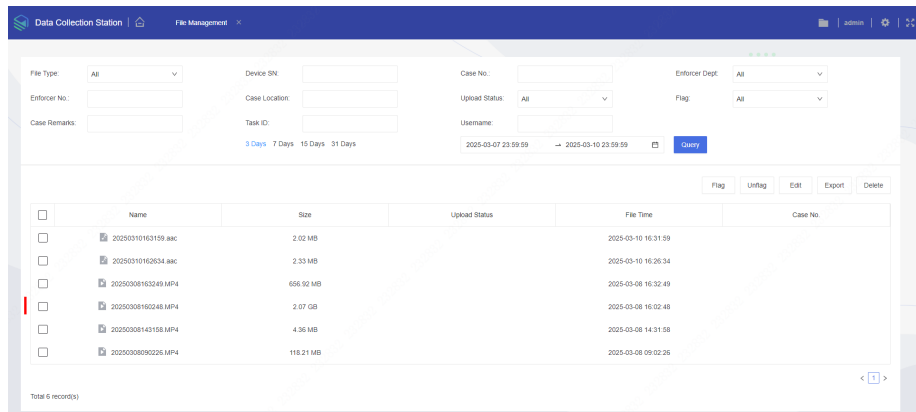
Procedure

- Step 1 Log in to the webpage of the Station, and then click  on the home page.
- Step 2 Select **File Management**, and then set file query conditions, such as **File Type**, **Upload Status**, **Device SN** and **Task ID**.



The maximum time range for file searching is 1 month.

Figure 3-61 File Management



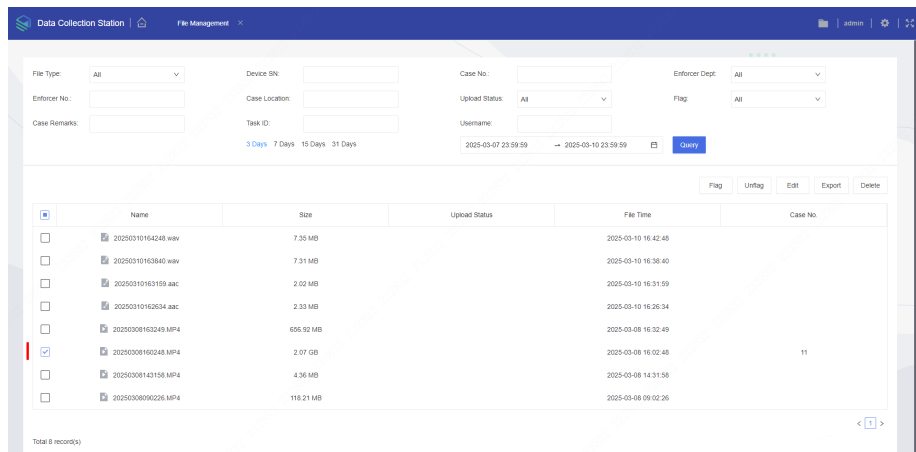
- Step 3 Click **Query**.

Related Operations

Support operations such as flagging, editing, and exporting searched files.

- Flag: Flag the file. You can add case NO., case location, and case remarks.

Figure 3-62 Flag



- Unflag: Unflag the file.
- Edit: Modify the case NO., case location, and case remarks.
- Export: Configure the export settings, such as storage path, and then export the file to the local location.

Figure 3-63 Export

The 'Export' dialog box contains the following fields and options:

- Picture :** ☒ Original
- Audio :** ☒ Original ☐ aac ☐ wav
- Video :** ☒ Original ☐ mp4 ☐ dav ☐ avi
- Storage Path :** C:\RecordDownload
-

- Delete: Delete the file.

3.2.3.3 Viewing Files

Double-click a file to view the details. Videos and images support full screen, partial magnification, and capture operations.



When viewing the video or audio, install the plug-in according to the notice on the webpage.

3.2.4 Log

Query and download local log, device log, collection log, and upload log.

3.2.4.1 Local Log

Procedure

- Step 1** Log in to the webpage of the Station, click  on the home page, and then select **Setting > Log > Local Log**.

Figure 3-64 Local Log

The screenshot shows the 'Local Log' page with a sidebar on the left containing links to Local Log, Device Log, Collection Log, and Upload Log. The main area has a 'Type' dropdown set to 'All', a time range selector from '2023-05-07 23:59:59' to '2023-06-06 23:59:59', and buttons for 'Query' and 'Backup'. Below is a table of log entries:

No.	Type	Time	Details
1	Playback	2023-06-06 11:56:42	Details
2	Account	2023-06-06 11:55:30	Details
3	Account	2023-06-06 11:55:30	Details
4	Account	2023-06-06 11:55:30	Details
5	Account	2023-06-06 11:55:30	Details
6	Account	2023-06-06 11:55:26	Details
7	Account	2023-06-06 11:55:26	Details
8	Account	2023-06-06 11:55:25	Details
9	Account	2023-06-06 11:55:25	Details
10	Account	2023-06-06 11:55:05	Details
11	Account	2023-06-06 11:55:05	Details
12	Account	2023-06-06 11:55:01	Details
13	Account	2023-06-06 11:55:01	Details
14	Account	2023-06-06 11:54:59	Details
15	Account	2023-06-06 11:54:59	Details

- Step 2** Select the type and set the query cycle.

- Step 3** Click **Query**.

The home page displays log files meeting the query conditions.

Related Operations

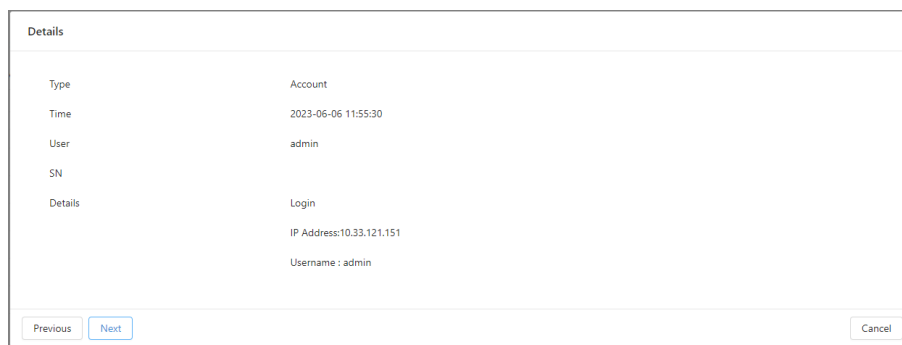
- Download log.

Click **Backup** to download the log to the computer. You can set the backup password as needed.

- View Details.

Click  to view the log details. Click **Previous** or **Next** to browse the log details.

Figure 3-65 Details



The 'Details' window displays the following information:

Type	Account
Time	2023-06-06 11:55:30
User	admin
SN	
Details	Login
	IP Address:10.33.121.151
	Username : admin

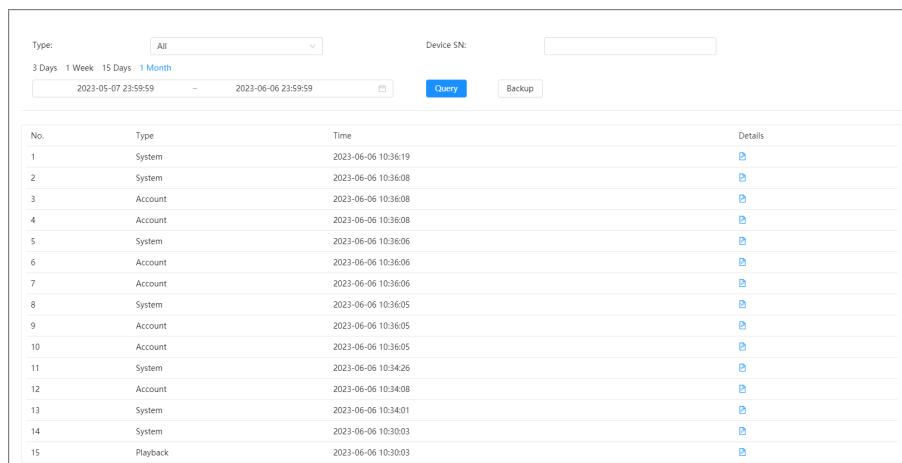
At the bottom, there are buttons for 'Previous', 'Next', and 'Cancel'.

3.2.4.2 Device Log

Procedure

- Step 1** Log in to the webpage of the Station, click  on the home page, and then select **Setting > Log > Device Log**.

Figure 3-66 Device Log



The 'Device Log' page includes a search filter section at the top with 'Type' set to 'All', a 'Device SN' input field, and a date range from '2023-05-07 23:59:59' to '2023-06-06 23:59:59'. There are 'Query' and 'Backup' buttons.

No.	Type	Time	Details
1	System	2023-06-06 10:36:19	
2	System	2023-06-06 10:36:08	
3	Account	2023-06-06 10:36:08	
4	Account	2023-06-06 10:36:08	
5	System	2023-06-06 10:36:06	
6	Account	2023-06-06 10:36:06	
7	Account	2023-06-06 10:36:06	
8	System	2023-06-06 10:36:05	
9	Account	2023-06-06 10:36:05	
10	Account	2023-06-06 10:36:05	
11	System	2023-06-06 10:34:26	
12	Account	2023-06-06 10:34:08	
13	System	2023-06-06 10:34:01	
14	System	2023-06-06 10:30:03	
15	Playback	2023-06-06 10:30:03	

- Step 2** Configure the query conditions.
Supports searching by type, device SN, and query cycle.

- Step 3** Click **Query**.
The home page displays log files meeting the query conditions.

Related Operations

- Download log.

Click **Backup** to download the log to the PC. You can set the backup password as needed.

- View Details.

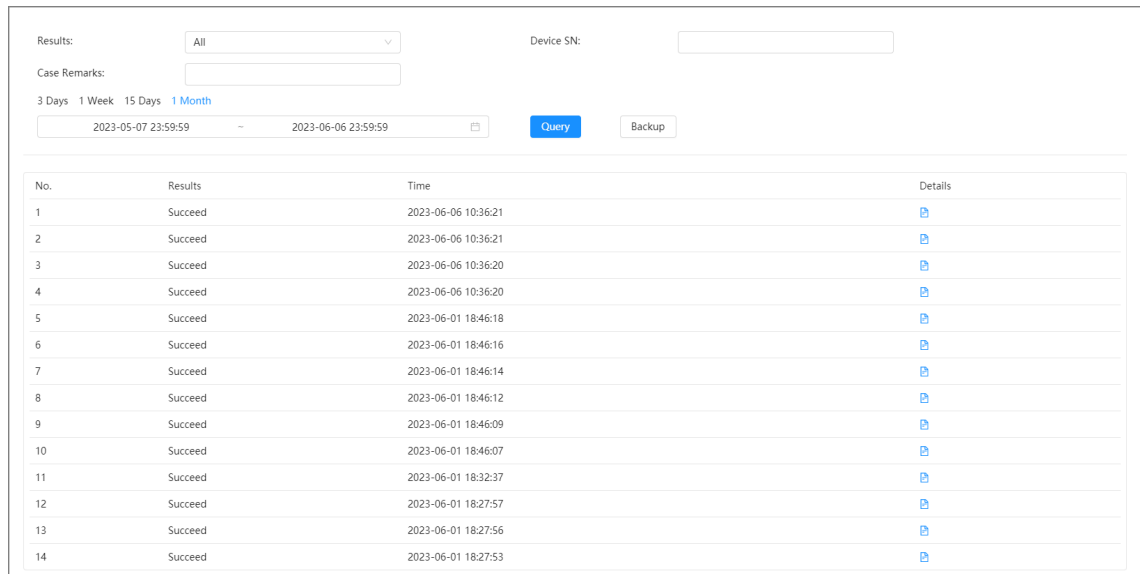
Click  to view the log details. Click **Previous** or **Next** to browse the log details.

3.2.4.3 Collection Log

Procedure

- Step 1** Log in to the webpage of the Station, click  on the home page, and then select **Setting > Log > Collection Log**.

Figure 3-67 Collection Log



The screenshot displays the 'Collection Log' interface. At the top, there are search filters: 'Results' (set to 'All'), 'Device SN:' (empty), and 'Case Remarks:' (empty). Below these are time range filters: '3 Days', '1 Week', '15 Days', and '1 Month' (selected). A date range is shown as '2023-05-07 23:59:59' to '2023-06-06 23:59:59'. There are 'Query' and 'Backup' buttons. The main area is a table with 14 rows of log entries.

No.	Results	Time	Details
1	Succeed	2023-06-06 10:36:21	
2	Succeed	2023-06-06 10:36:21	
3	Succeed	2023-06-06 10:36:20	
4	Succeed	2023-06-06 10:36:20	
5	Succeed	2023-06-01 18:46:18	
6	Succeed	2023-06-01 18:46:16	
7	Succeed	2023-06-01 18:46:14	
8	Succeed	2023-06-01 18:46:12	
9	Succeed	2023-06-01 18:46:09	
10	Succeed	2023-06-01 18:46:07	
11	Succeed	2023-06-01 18:32:37	
12	Succeed	2023-06-01 18:27:57	
13	Succeed	2023-06-01 18:27:56	
14	Succeed	2023-06-01 18:27:53	

- Step 2** Configure the query conditions.

Supports searching by results, device SN, case remarks, and query cycle.

- Step 3** Click **Query**.

The home page displays log files meeting the query conditions.

Related Operations

- Download log.
Click **Backup** to download the log to the PC. You can set the backup password as needed.
- View Details.

Click  to view the log details. Click **Previous** or **Next** to browse the log details.

3.2.4.4 Upload Log

Procedure

- Step 1** Log in to the webpage of the Station, click  on the home page, and then select **Setting > Log > Upload Log**.

Figure 3-68 Upload Log

Results: All

Case No.:

3 Days 1 Week 15 Days 1 Month

2023-05-07 23:59:59 ~ 2023-06-06 23:59:59

Device SN:

Case Remarks:

Upload Mode: All

Query

Backup

No.	Results	Time	Details
1	Succeed	2023-05-30 10:18:13	Details
2	Succeed	2023-05-30 10:18:13	Details
3	Succeed	2023-05-30 10:17:59	Details
4	Succeed	2023-05-30 10:16:28	Details
5	Succeed	2023-05-30 10:15:44	Details
6	Succeed	2023-05-30 10:15:40	Details
7	Succeed	2023-05-30 10:15:12	Details
8	Succeed	2023-05-30 10:12:28	Details
9	Succeed	2023-05-30 10:04:15	Details
10	Succeed	2023-05-30 09:57:52	Details
11	Succeed	2023-05-30 09:57:42	Details
12	Succeed	2023-05-30 09:57:37	Details
13	Succeed	2023-05-30 09:57:37	Details
14	Succeed	2023-05-30 09:57:36	Details

Step 2 Configure the query conditions.

Support searching by results, upload mode, device SN, case No., case remarks, and query cycle.

Step 3 Click **Query**.

The home page displays log files meeting the query conditions.

Related Operations

- Download log.

Click **Backup** to download the log to the PC. You can set the backup password as needed.

- View Details.

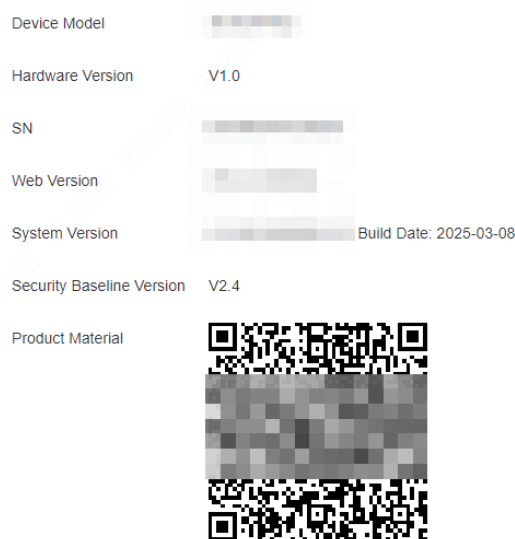
Click [Details](#) to view the log details. Click **Previous** or **Next** to browse the log details.

3.2.5 Settings

3.2.5.1 System Information

Log in to the webpage of the Station, click [Settings](#) on the home page, select **Maintenance Center** > **System Info**, and then view the device model, hardware version, SN, and other system information.

Figure 3-69 System information



3.2.5.2 System Update



- During the update, do not power off, restart, shut down the station, or disconnect it from the network.
 - Make sure that the update file is correct. Improper upgrade file might result in device error.
1. Log in to the webpage of the Station, click  on the home page, select **Maintenance Center** > **Update**, click **Browse**, and then select the upgrade file of type. bin to upgrade.
 2.
 - Auto update
Enable **Auto Update**. When the body camera connects to the collection station, it will automatically detect files and update them.
 - Upload update files
 - a. Browse to the storage path on your computer and select the corresponding body camera upgrade package.
 - b. Click **Upload**.Once the upload is successful, it will be displayed in the list below, and you can click **Delete** to remove the corresponding upgrade file.

Figure 3-70 Update

File Update

Path

Device Update

Auto Update ☐

Please do not change the original name of the update package when uploading it.

Model	Uploaded Update Package Version	Delete

3.2.5.3 Log Running

Select **Setting** > **Maintenance Center** > **Run Log**.



The file needs to be decrypted before it can be viewed after downloading.

- Exporting the collection station logs: Enable **Print Log** and click **Apply**. This will start recording the device's debug-level operating logs, with the log file name and file size displayed in the list below. Select the checkbox next to the log file you wish to export, and click **Download** to download the log file to your computer for troubleshooting purposes.
- Exporting MPT logs: Click **Slot Selection**, choose the slot where the recorder for which you want to export logs is located, and click **Export**. This will download the operating logs of the selected recorder to your computer.

Figure 3-71 Run log

Data Collection Station | File Management | Setting

Maintenance Cen... > Run Log

Log Export for EEC Device

Print Log ☐

☐	File Name	Size(KB)	Download

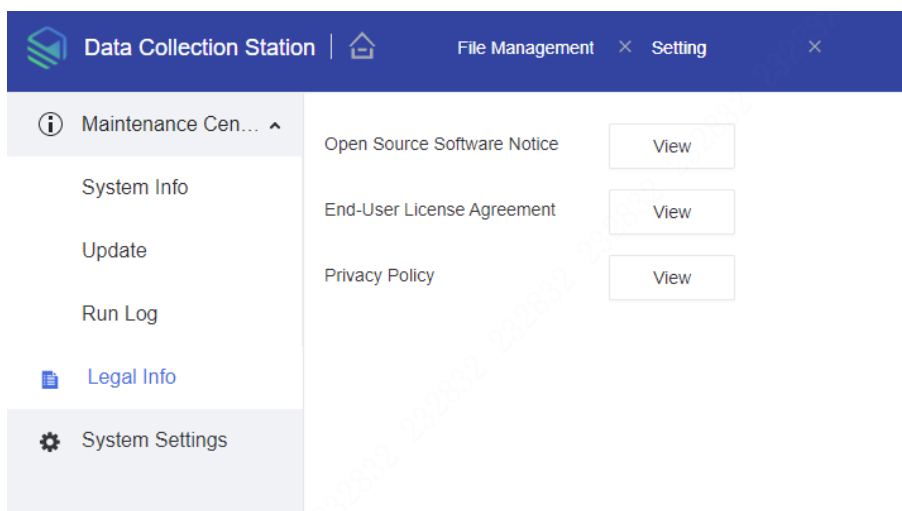
Log Export for MPT Devices

Slot Selection

3.2.5.4 Legal Information

Log in to the webpage of the Station, click  on the home page, select **Maintenance Center** > **Legal Info**, and then click **View** to view the open source software notice, end-user license agreement, and privacy policy.

Figure 3-72 Legal Info

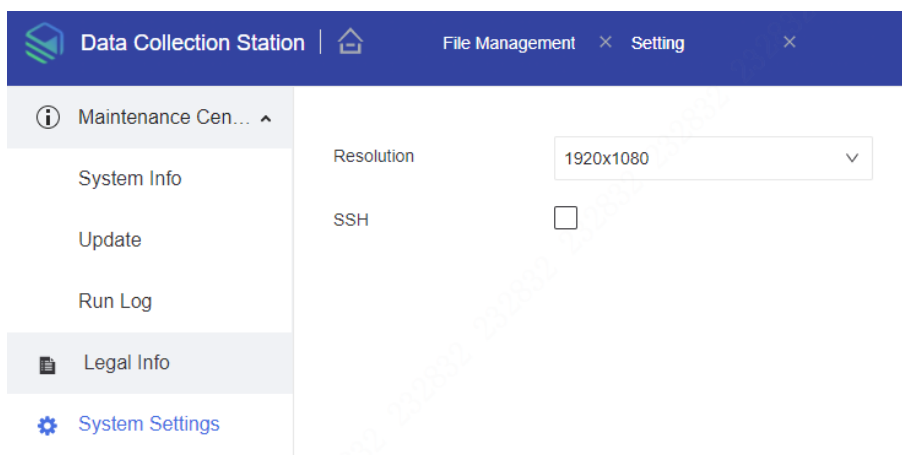


3.2.5.5 System Settings

Log in to the webpage of the Station, click  on the home page, and then select **Maintenance Center** > **System Settings**.

Set **Resolution**, select **SSH**, and then click **Enter**.

Figure 3-73 System Settings



Appendix 1 Security Recommendation

Account Management

1. Use complex 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: 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 repeating characters, such as 111, aaa, etc.

2. Change passwords periodically

It is recommended to periodically change the device password to reduce the risk of being guessed or cracked.

3. Allocate accounts and permissions appropriately

Appropriately add users based on service and management requirements and assign minimum permission sets to users.

4. Enable account logout function

The account logout function is enabled by default. You are advised to keep it enabled to protect account security. After multiple failed password attempts, the corresponding account and source IP address will be locked.

5. Set and update password reset information in a timely manner

The device supports password reset function. To reduce the risk of this function being used by threat actors, if there is any change in the information, please modify it in time. When setting security questions, it is recommended not to use easily guessed answers.

Service Configuration

1. Enable HTTPS

It is recommended that you enable HTTPS to access web services through secure channels.

2. Encrypted transmission of audio and video

If your audio and video data contents are very important or sensitive, it is recommended to use encrypted transmission function in order to reduce the risk of your audio and video data being eavesdropped during transmission.

3. Turn off non-essential services and use safe mode

If not needed, it is recommended to turn off some services such as SSH, SNMP, SMTP, UPnP, AP hotspot etc., to reduce the attack surfaces.

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

- SNMP: Choose SNMP v3, and set up strong encryption and authentication passwords.
- SMTP: Choose TLS to access mailbox server.
- FTP: Choose SFTP, and set up complex passwords.
- AP hotspot: Choose WPA2-PSK encryption mode, and set up complex passwords.

4. Change HTTP and other default service ports

It is recommended that you change the default port of HTTP and other services to any port between 1024 and 65535 to reduce the risk of being guessed by threat actors.

Network Configuration

1. **Enable Allowlist**

It is recommended that you turn on the allowlist function, and only allow IP in the allowlist to access the device. Therefore, please be sure to add your computer IP address and supporting device IP address to the allowlist.

2. **MAC address binding**

It is recommended that you bind the IP address of the gateway to the MAC address on the device to reduce the risk of ARP spoofing.

3. **Build a secure network environment**

In order to better ensure the security of devices and reduce potential cyber risks, the following are recommended:

- Disable the port mapping function of the router to avoid direct access to the intranet devices from external network;
- According to the actual network needs, partition the network: if there is no communication demand between the two subnets, it is recommended to use VLAN, gateway and other methods to partition the network to achieve network isolation;
- Establish 802.1x access authentication system to reduce the risk of illegal terminal access to the private network.

Security Auditing

1. **Check online users**

It is recommended to check online users regularly to identify illegal users.

2. **Check device log**

By viewing logs, you can learn about the IP addresses that attempt to log in to the device and key operations of the logged users.

3. **Configure network log**

Due to the limited storage capacity of devices, the stored log is limited. If you need to save the log for a long time, it is recommended to enable the network log function to ensure that the critical logs are synchronized to the network log server for tracing.

Software Security

1. **Update firmware in time**

According to the industry standard operating specifications, the firmware of devices needs to be updated to the latest version in time in order to ensure that the device has the latest functions and security. If the device is connected to the public network, it is recommended to enable the online upgrade automatic detection function, so as to obtain the firmware update information released by the manufacturer in a timely manner.

2. **Update client software in time**

It is recommended to download and use the latest client software.

Physical Protection

It is recommended that you carry out physical protection for devices (especially storage devices), such as placing the device in a dedicated machine room and cabinet, and having access control

and key management in place to prevent unauthorized personnel from damaging hardware and other peripheral equipment (e.g. USB flash disk, serial port).