

Data Collection Station

User Manual



V2.1.0

Foreword

General

This manual introduces the functions and operations of the data collection station (hereinafter referred to as "the Station").

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
V2.1.0	Updated figures in "4.1.4 Local Settings".	May 2025
V2.0.0	- Updated figures in "4.1.4 Local Settings". - Added "4.1.5 Platform Configuration" and "4.1.4.6.3 Attack Defense".	November 2021
V1.0.1	Updated "1.1 Introduction".	May 2021
V1.0.0	First release.	March 2021

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.

Important Safeguards and Warnings

This section introduces content covering the proper handling of the Device, hazard prevention, and prevention of property damage. Read carefully before using the Device, 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.
- To avoid short circuits caused by metal objects touching the battery anode and cathode, do not store the battery with other metals.
- If the device will not be used for a week or longer, charge it to 60%, take the battery out of the device, and store it in a clean, dry and ventilated room with an ambient temperature of 20 ± 5 °C.
- Charge the battery once every four months during storage.

Installation Requirements



- The Device must be installed in a location that only professionals can access. Non-professionals are not allowed to enter the installation area.
- The Device must be reliably grounded by professionals. They must install the grounding conductor in the building floor and verify the grounding connection of the output receptacle.
- When installing the Device, make sure that the power plug can be easily reached to cut off the power.
- Improper installation might cause harm to you or the device.
- If you are not sure how to install the stand, entrust the installation to professionals.
- If any part or component of the stand is damaged, do not install the stand.
- The stand is designed to support the data collection station. Do not use the stand for other purposes.
- Net weight: 55 kg; load bearing capacity: 100 kg. To ensure safety, do not use the stand to support a load exceeding its bearing capacity.
- If you are unaware of the load bearing capacity, do not install the stand.

Operation Requirements



-   The Device or remote control contains button batteries. Do not swallow the batteries due to the risk of chemical burns.

Possible result: The swallowed button battery can cause serious internal burns and death within 2 hours.

Preventive measures (including but not limited to):

- ◇ Keep new and used batteries out of reach of children.
 - ◇ If the battery compartment is not securely closed, stop using the product immediately and keep out of reach of children.
 - ◇ Seek immediate medical attention if a battery is believed to be swallowed or inserted inside any part of the body.
- Battery Pack Precautions

Preventive measures (including but not limited to):

- ◇ Do not transport, store or use the batteries in high altitudes with low pressure and environments with extremely high and low temperatures.
- ◇ Do not dispose the batteries in fire or a hot oven, or mechanically crush or cut the batteries to avoid an explosion.
- ◇ Do not leave the batteries in environments with extremely high temperatures to avoid explosions and leakage of flammable liquid or gas.
- ◇ Do not subject the batteries to extremely low air pressure to avoid explosions and the leakage of flammable liquid or gas.

WARNING

- Use the power adapter and cables provided with the device. We assume no responsibility for injuries or damage caused by using the incorrect power adapter and cables.

-  High Sound Pressure

Possible cause: Danger of hearing loss.

Preventive measure: Do not listen at high volume levels for long periods.



- Use the Device under allowed humidity and temperature conditions.
- Do not continuously charge the battery for 24 hours or longer. When it is finished charging or it no longer needs charging, disconnect the adapter from the device, and unplug it from the power socket.
- Please be advised that your configurations will be lost after performing a factory reset.

Maintenance Requirements

DANGER

Replacing unwanted batteries with the wrong type of new batteries might result in explosion.

Preventive measures (including but not limited to):

- Replace unwanted batteries with new batteries of the same type and model to avoid the risk of fire and explosion.
- Dispose of the old batteries as instructed.



The battery is a consumable accessory. We recommend replacing it after it has been used for a year.

Table of Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Overview.....	1
1.1 Introduction.....	1
1.2 Features.....	1
1.3 Product Appearance.....	2
1.3.1 Control Module.....	2
1.3.2 Appearance of Data Collection Modules.....	5
1.4 Description of Buttons.....	6
1.5 Power On.....	7
2 Device Connection.....	8
2.1 Connecting Control Module and Data Collection Module.....	8
2.2 Connecting Body Camera and Data Collection Module.....	8
3 HDD Installation.....	13
4 Configuration and Operation.....	17
4.1 General.....	17
4.1.1 Login.....	18
4.1.2 File Management.....	20
4.1.3 Searching for Logs.....	21
4.1.4 Local Settings.....	23
4.1.5 Platform Configuration.....	67
4.2 Web Configuration.....	70
4.2.1 Login.....	70
4.2.2 File Management.....	70
4.2.3 Configuring Web.....	72
Appendix 1 RAID.....	75
Appendix 2 Cybersecurity Recommendations.....	78

1 Overview

1.1 Introduction

Working with body camera, the Station can acquire the data of body cameras and charge them. The Station can auto recognize and connect the connected body camera through the USB port. Working with the platform, the Station can authorize the body camera, and auto acquire the electronic evidence (video, audio, and snapshot). The Station contains control module and data collection module. One control module can support 4 data collection modules at most.

1.2 Features

- Recharge and collect data from maximum 32 body cameras at the same time.
- Automatically or manually update body cameras.
- Automatically create archive and then save the collected electronic data.
- Automatically upload the evidence to FTP or the platform.
- Automatically synchronize time with the platform.
- When there are more than one data collection modules, the Station will collect data from the body camera in the fixed docks of each data collection module in priority.
- You can search, edit, transcode, play back, view, delete and manage all the data in the Station.

1.3 Product Appearance

1.3.1 Control Module

Figure 1-1 Front panel and rear panel

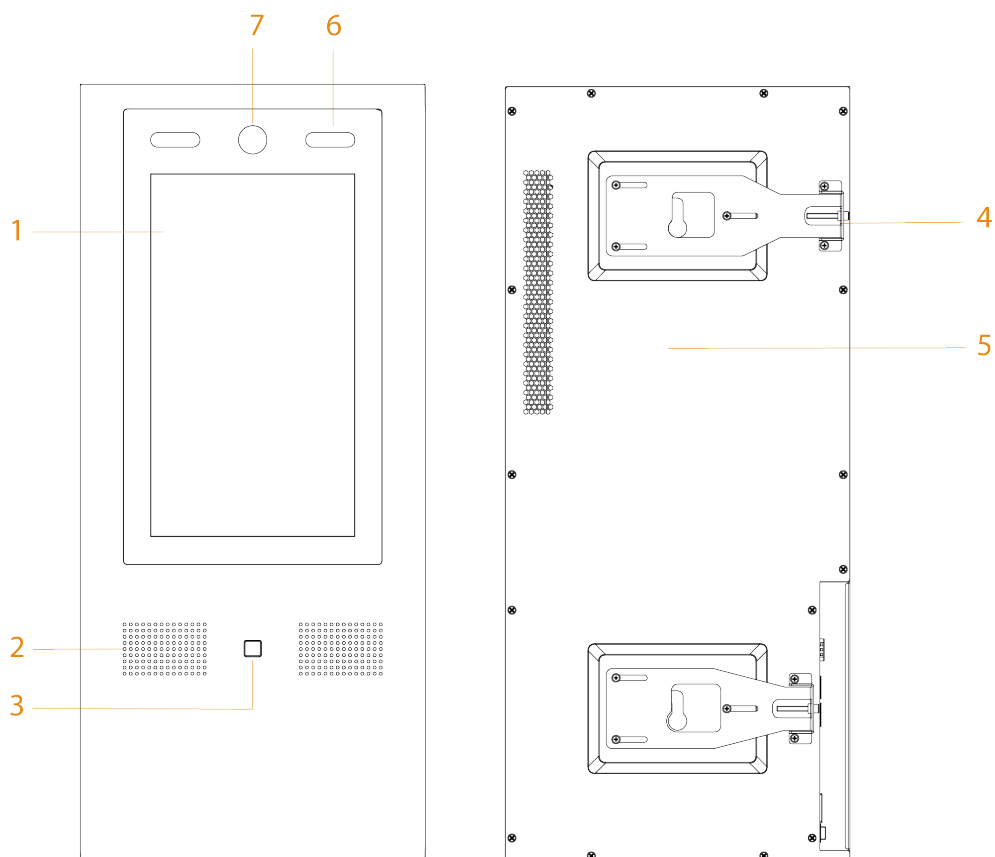


Figure 1-2 Side panel

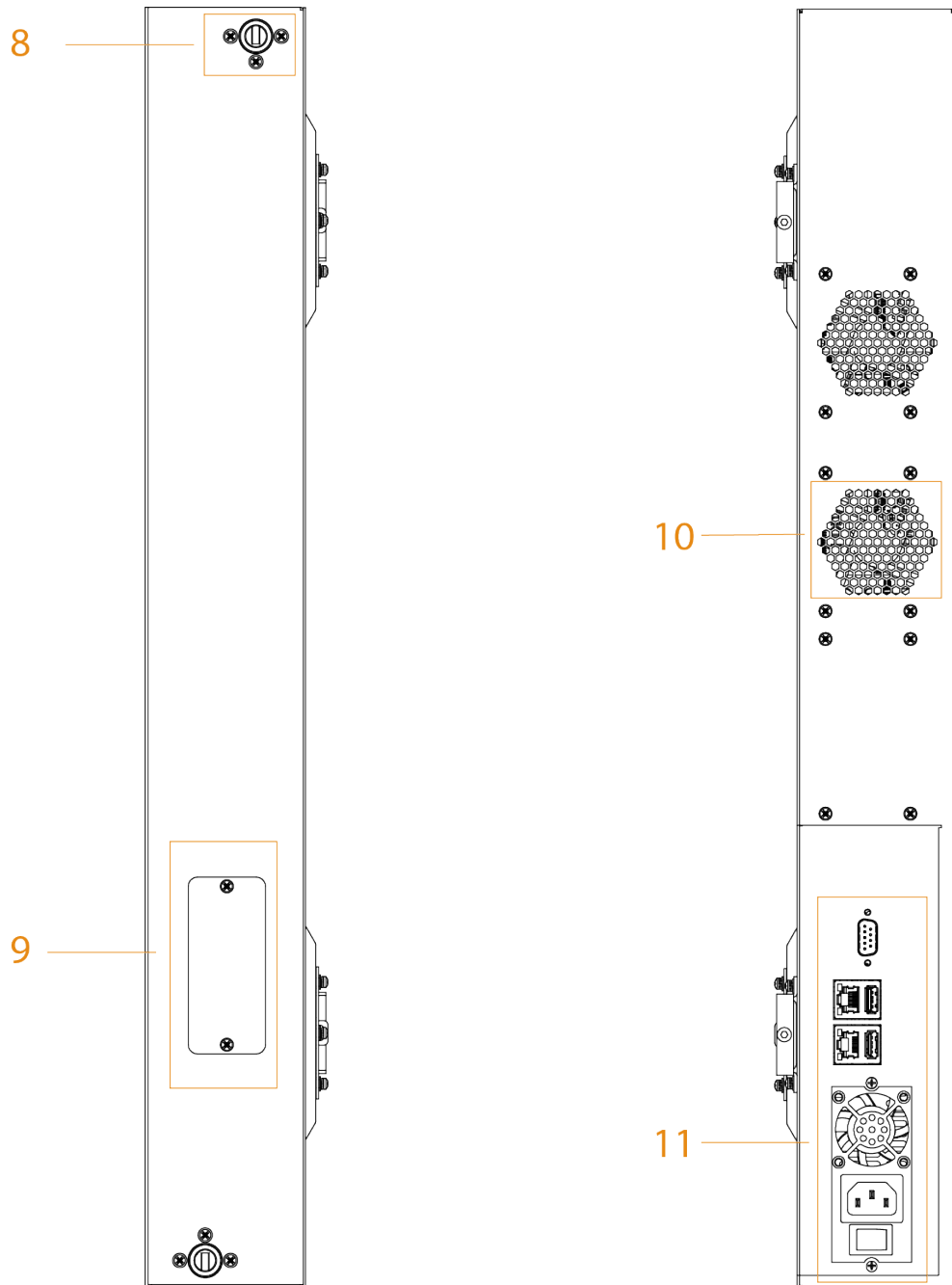


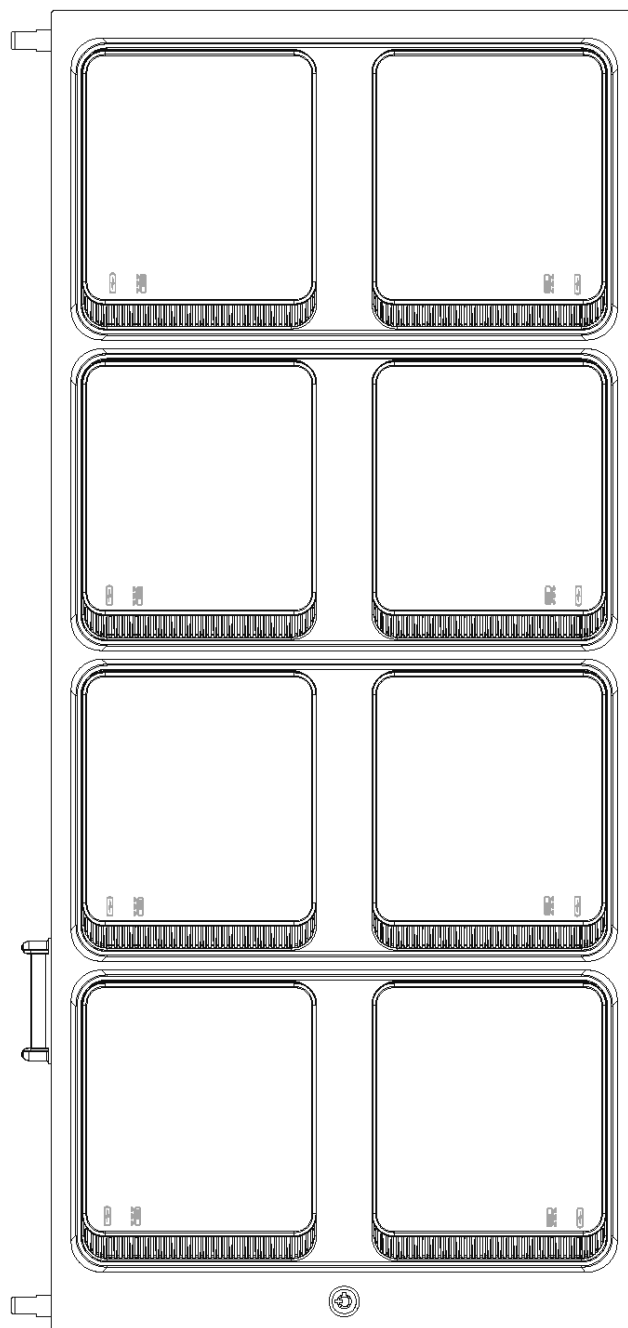
Table 1-1 Appearance description

No.	Name	Description
1	Touchscreen	13.3-inch touchscreen.
2	Speaker	Audio output.
3	Fingerprint sensor	• Add fingerprint data or unlock by fingerprint. • Up to 3 fingerprints can be added for each user.
4	Adjusting board	Remove the control module when connecting control module and data collection modules.

No.	Name	Description
5	Rear cover	—
6	White light	• Provides extra light when recognizing faces. • Provides extra light to the camera in dark condition.
7	Camera	Recognizes face information. You can unlock the Station through face recognition.
8	Axle housing	Connects the control module and data collection modules. One is at the top, and the other is at the bottom.
9	Connector	Transfers the data from control module and data collection modules.
10	Heat dissipation hole	—
11	Ports	Include power input port, USB ports, Ethernet ports, and RS-232 port. For details, see "1.4 Description of Buttons".

1.3.2 Appearance of Data Collection Modules

Figure 1-3 Appearance of data collection modules



- Put body cameras into docks for data collection. When there are more than one data collection modules, the data of the body cameras in the two docks of the first row will be collected first.

- There are two icons below a dock:  indicates recharging;  indicates collecting data.
- When a dock cannot be opened, you can open it with the key.
- In data collection, the indicator light flashes blue; When data collection is complete, it shows a constant blue.

1.4 Description of Buttons

Figure 1-4 Ports

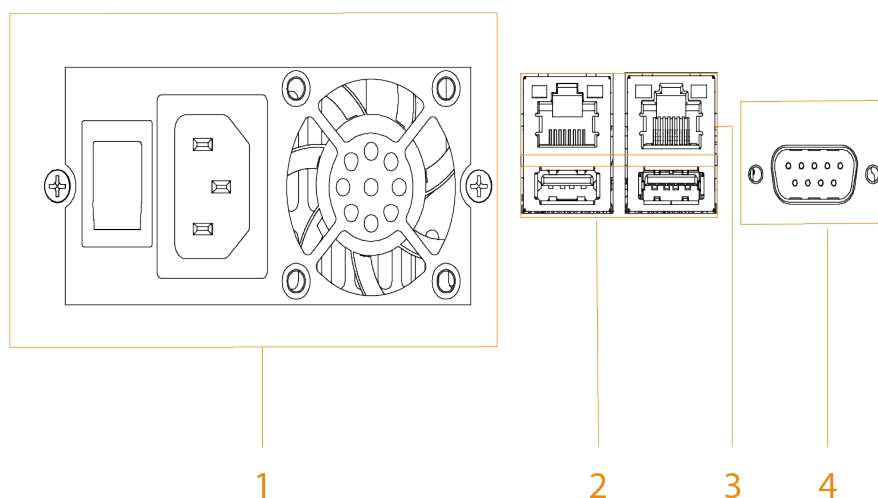


Table 1-2 Port description

No.	Name	Description
1	Power input	Inputs 100–240 VAC power for the Station.  After shutting down the Station, the fan will work for a period to cool the Station.
2	USB ports	Connect to USB storage devices (USB 2.0 and USB 3.0), mouse, and more.
3	Ethernet	2 Gigabit ports.  When you use two ports at the same time, only one port can obtain the gateway automatically. For the other Ethernet card, disable the function of obtaining IP address automatically.
4	RS-232	Used for common serial debugging, IP address configuration and data transmission of transparent serial.

1.5 Power On

Procedure

Step 1 Connect the power cable and network cable.

Step 2 Press the power button.

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



The cover of the Station has static electricity, which might cause electric shock. To avoid electric shock, make sure the Station is well grounded.

2 Device Connection

2.1 Connecting Control Module and Data Collection Module

Procedure

- Step 1 Fix the control module on the wall.
- Step 2 Stick the positioning map of data collection module on the wall.
- Step 3 Fix the data collection module according to the instruction on the positioning map.



- You can connect 4 data collection modules to the control module at most.
- For the installation details, see the instructions on the positioning map.

2.2 Connecting Body Camera and Data Collection Module

Background Information

After starting the Station, connect body cameras to the Station, and then you can collect data from body cameras and recharge them.



Make sure that the connection of body cameras and data collection module is proper, and the body cameras are placed in slots correctly. If the body cameras are not placed in slots properly, the cameras might drop when docks open, or the docks cannot be opened.



The slots are designed exclusively for MPT220 and MPT230 body cameras by default. If you want to use them for MPT210 body camera, use the separate slot in the accessories package.

Procedure

- Step 1 Open the dock through the touch screen or the key, and then take out the data cable.



Do not violently pull data cable. Otherwise, it might result in invalid spring or loosening port connection.

Figure 2-1 Take out data cable (MPT220 slot)



Figure 2-2 Take out data cable (MPT210 slot)



Step 2 Connect the data cable to the body camera until the Station pops up the connection successful dialog box.

Figure 2-3 Connect device (MPT220 slot)



Figure 2-4 Connect device (MPT210 slot)



Step 3 After the connection, put the body camera into the dock, and then you can collect data and recharge the body camera.



- For the MPT 220 body camera, insert the device into the slot.

Figure 2-5 Data collection (MPT220 slot)



- For the MPT 210 body camera, insert the clip into the slot. Only MPT210 body camera with the latest clip can be inserted into the slot.

Figure 2-6 Data collection (MPT210 slot)



- For the MPT 230 body camera, insert the device into the slot.

Figure 2-7 Data collection (MPT230 slot)



3 HDD Installation

Background Information

You can install six 10T HDDs (hard disk drives).

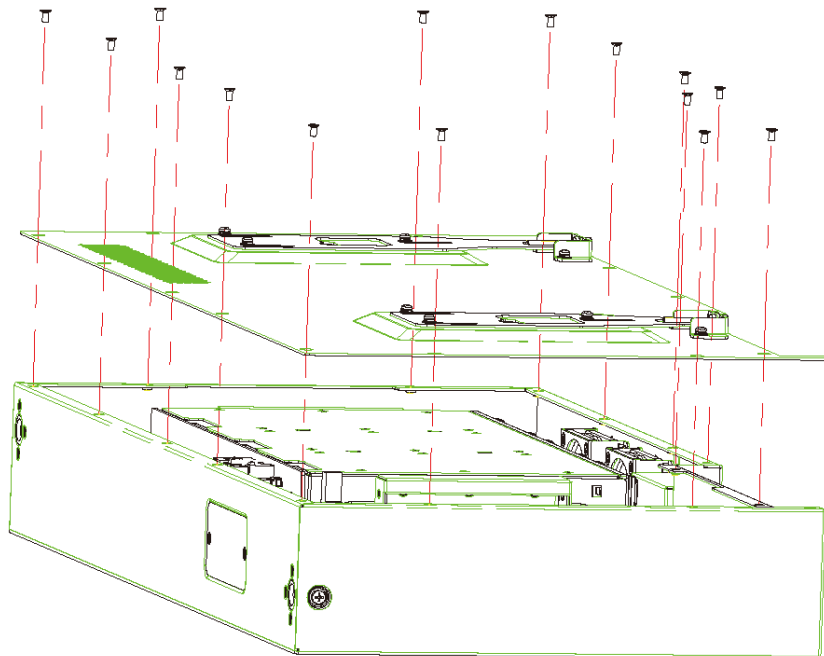


- To avoid insufficient storage space, HDDs larger than 2T are recommended.
- To reduce the writing pressure of each HDD, we recommend you to install at least 2 HDDs with the same capacity for data collection and recharging.

Procedure

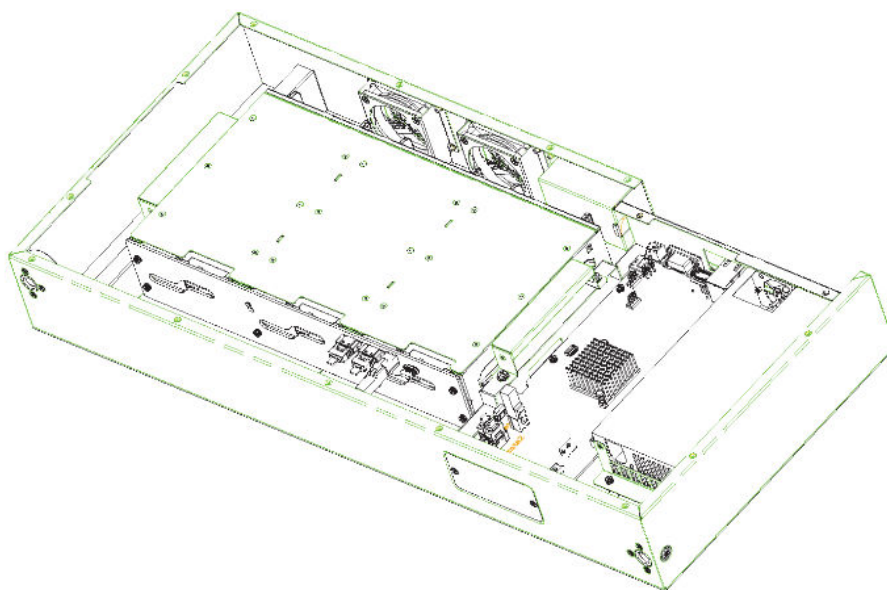
Step 1 Loosen the screws on the rear cover, and then remove the rear cover.

Figure 3-1 Remove rear cover



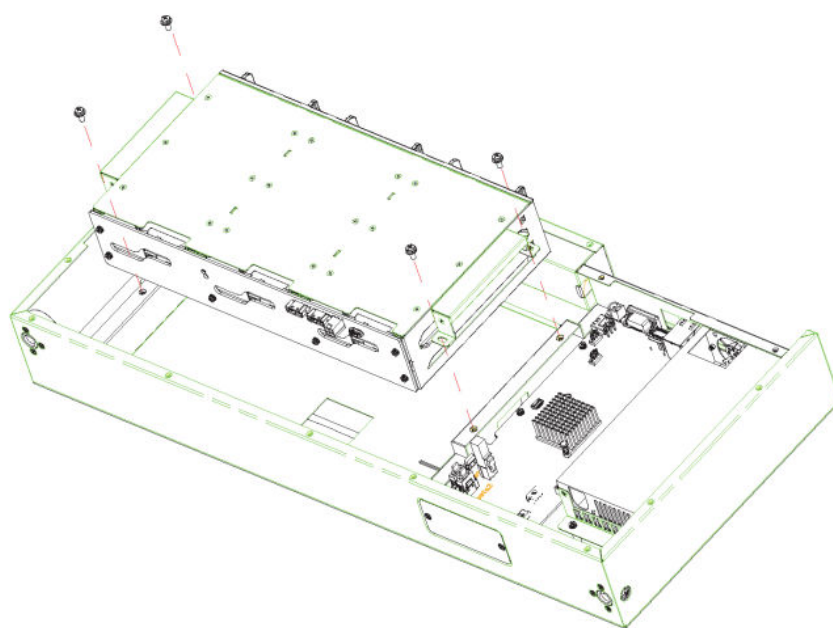
Step 2 Disconnect the cables between main board and HDD plate.

Figure 3-2 Loosen cable



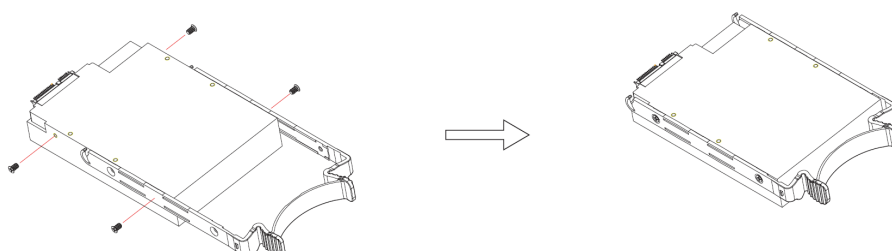
Step 3 Loosen the four fixed screws on the HDD box, and then take out the box.

Figure 3-3 Take out HDD box



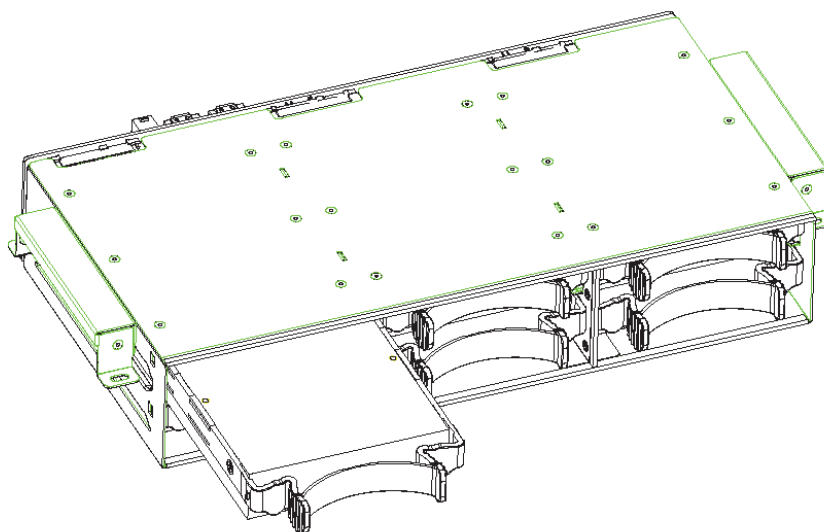
Step 4 Fix HDDs.

Figure 3-4 Fix HDD



Step 5 Install HDDs. Push the fixed HDDs in the HDD box.

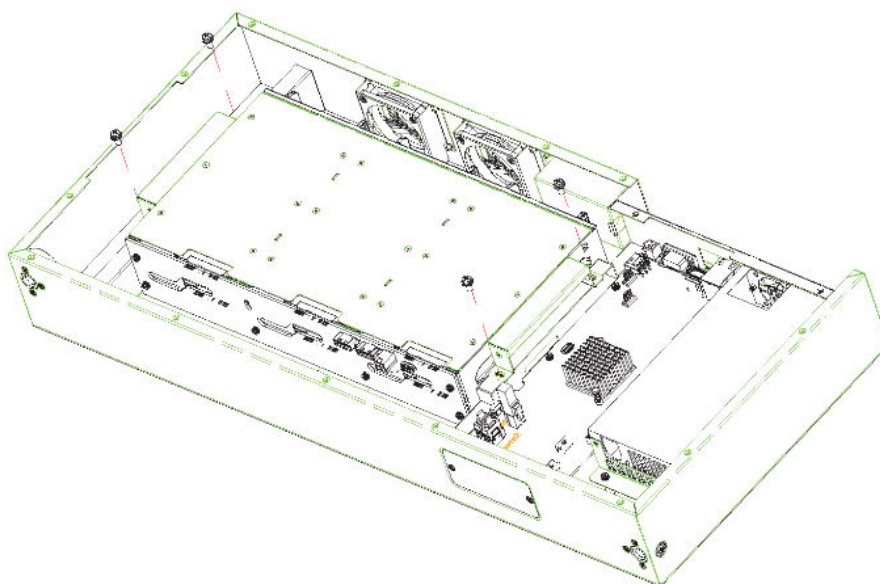
Figure 3-5 Install HDD



Push HDDs in the direction as the HDD port and main board port show.

Step 6 Fix the HDD box in the chassis.

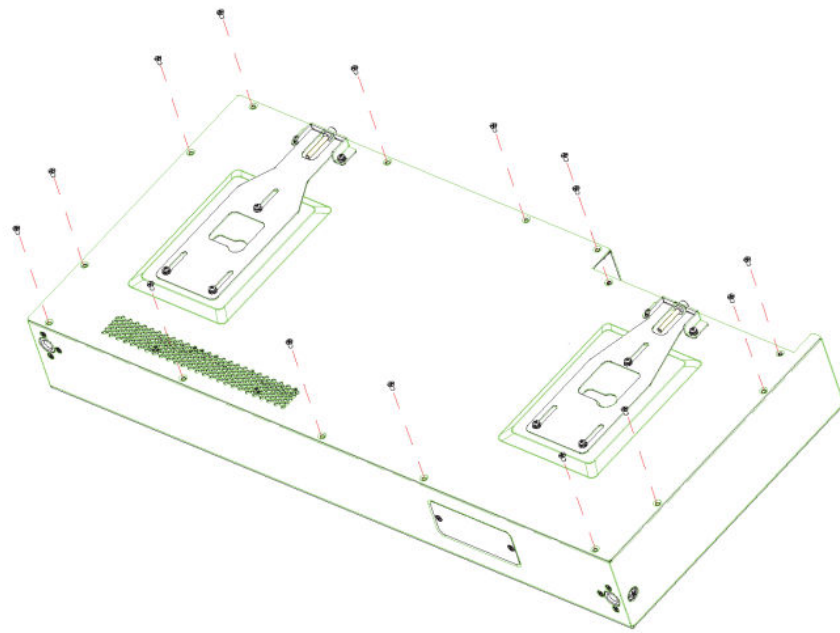
Figure 3-6 Install HDD box



Step 7 Connect the cable between main board and HDD plate.

Step 8 Fix the cover.

Figure 3-7 Fix the cover



4 Configuration and Operation

4.1 General

Figure 4-1 Home screen

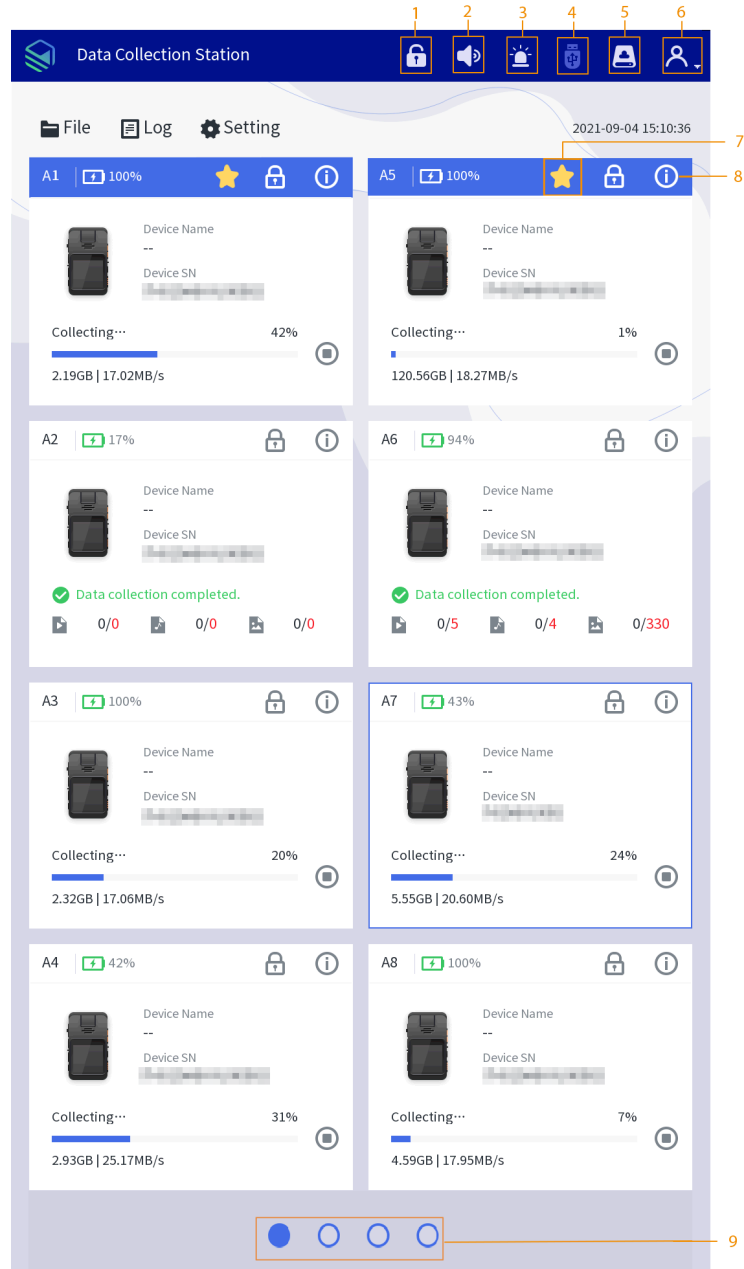


Table 4-1 Home screen description

No.	Description
1	Unlock the dock by one tap.
2	Alarm. Tap it, and the alarm tune is disabled.
3	Alarm information display. The red light flashes when there is alarm.

No.	Description
4	External USB storage device. Grey means no USB storage device is connected.
5	View HDD capacity.
6	Login, logout, restart, shutdown, and editing the user information.
7	 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.
8	View update methods of the Station and body cameras.  Tap Bind Enforce on the Device Info screen, enter the enforcer name and enforcer No., tap Search , and then select the enforcer that you want to bind.
9	Switch screens of data collection modules. It supports 4 screens at most.

4.1.1 Login



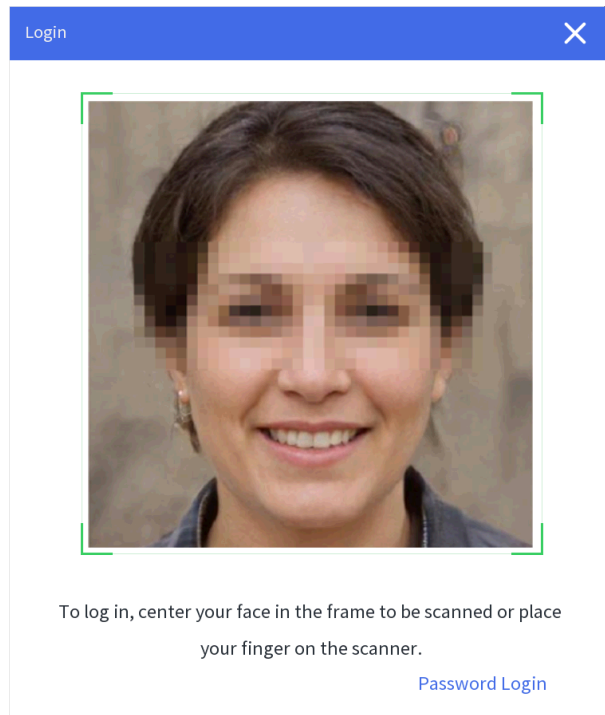
Before using face login or fingerprint login, you need to complete related configurations. For details, see "4.1.4.1 User".

Face Login

After the Station starts, place your face in the detection frame.

After unlocked, the Station displays the home screen.

Figure 4-2 Face login



Fingerprint Login

After the Station starts, place your finger on the scanner.

After unlocked, the Station displays the home screen.

Password Login

After the Station starts, tap **Password Login** on the lower-right corner of the **Login** screen, and then enter username and password.

After unlocked, the Station displays the home screen.

Figure 4-3 Password login

4.1.2 File Management

4.1.2.1 File Collection

After collecting data files from body cameras, the Station will upload the files to the platform according to the configuration in **Storage**.

4.1.2.2 Searching for Files

You can search for video files, audio files and snapshots according to the configured conditions, including file type, enforcer department, upload status, device SN, enforcer No, flag, case No., case location, case remarks, start time, end time, task ID and username.

- 1. Click **File** in the home page.
- 2. Configure the file type, device SN and other query conditions.



The maximum time range for file searching is 1 month.

Figure 4-4 Searching for files

File

File Type

All

Device SN

Case No.

Enforcer Dept

All

Enforcer No.

Case Location

Upload Status

All

Flag

All

Case Remarks

Task ID

Username

3 Days

7 Days

15 Days

31 Days

2025-03-07 23:59:59

-

2025-03-10 23:59:59

Query

★ Flag

☆ Unflag

✎ Edit

📄 Export

🗑 Delete

☐	Name	Size	Upload	Time	Case No.
☐	20250310163159.aac	2.03 MB		2025-03-10 16:31:59	
☐	20250310162634.aac	2.33 MB		2025-03-10 16:26:34	
☐	20250308163249.MP4	656.92 MB		2025-03-08 16:32:49	
☐	20250308160248.MP4	2.08 GB		2025-03-08 16:02:48	
☐	20250308143158.MP4	4.36 MB		2025-03-08 14:31:58	
☐	20250308090226.MP4	118.21 MB		2025-03-08 09:02:26	

Total

6

record(s)

<

1/1

>

Goto

1

Page

➔

- 3. Click **Query**.

The page displays files that meet the query conditions and supports operations such as flagging, unflagging, editing, exporting and deleting the files.

4.1.2.3 Viewing Files

Double-tap a file to view the details, and you can do the operations of fast play, slow play, zoom in or zoom out.



You cannot fast play or slow play an audio file in AMR format.

4.1.3 Searching for Logs

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

4.1.3.1 Local Log

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



The maximum time range for log searching is 1 month.

Figure 4-5 Local log

The screenshot shows the 'Log' application interface. On the left is a sidebar with four options: 'Local Log' (selected), 'Device Log', 'Collection Log', and 'Upload Log'. The main area has a search filter section with a 'Type' dropdown set to 'All', radio buttons for '3 Days', '7 Days', '15 Days', and '31 Days', and a 'Backup' button. Below these are two date-time pickers showing '2025-03-17 23:59:59' and '2025-03-20 23:59:59', followed by a 'Query' button. The results are displayed in a table with columns: No., Type, Time, and Details. The table contains six entries, all of which are 'MPT Operation' logs. At the bottom, there is a pagination bar showing 'Total 23783 record(s)', navigation arrows, '1/1586', a 'Goto' field with '1', and a 'Page' field with a right arrow.

No.	Type	Time	Details
1	Account	2025.03.20 20:51:08	
2	MPT Operation	2025.03.20 20:50:46	
3	MPT Operation	2025.03.20 20:50:45	
4	MPT Operation	2025.03.20 20:49:52	
5	MPT Operation	2025.03.20 20:49:52	
6	MPT Operation	2025.03.20 20:49:46	

Total 23783 record(s) 1/1586 Goto 1 Page

4.1.3.2 Device Log

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



The maximum time range for log searching is 1 month.

Figure 4-6 Device log

No.	Type	Time	Details
Total 0 record(s)			

4.1.3.3 Collection Log

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



The maximum time range for log searching is 1 month.

Figure 4-7 Collection log

No.	Results	Time	Details
Total 0 record(s)			

4.1.3.4 Upload Log

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



The maximum time range for log searching is 1 month.

Figure 4-8 Upload log

4.1.4 Local Settings

4.1.4.1 User

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

4.1.4.1.1 User Management

Procedure

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

Figure 4-9 User management

Step 2 Tap **Add** to add users.

You can add faces and fingerprints, and configure user permissions. All permissions are enabled by default.

Figure 4-10 Add users

The screenshot shows a modal window titled "Add" with a close button (X) in the top right corner. The form contains the following elements:

- Username:** A text input field with the value "abc" displayed to its right.
- Password:** A text input field with masked characters (dots).
- Confirm Password:** A text input field with masked characters (dots).
- Password Hint:** A text block stating: "Password must be 8 to 32 characters, including at least two of the following categories: numbers, uppercase letters, lowercase letters and special characters (Characters like ' ' ; : & cannot be included in)."
- Face:** A button labeled "+ Add".
- Fingerprint:** A button labeled "+ Add".
- Permission:** A section with a list of permissions, each preceded by a checked checkbox:
 - ☒ All
 - ☒ SYSTEM INFO
 - ☒ Export File
 - ☒ FILE MANAGEMENT
 - ☒ System Settings
 - ☒ ACCOUNT
 - ☒ Unlock All
- Buttons:** "OK" and "Back" buttons at the bottom right.

4.1.4.1.2 Enforcer Management

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

Adding Enforcer

Tap **Add** to add users. Enter enforcer department, enforcer No., enforcer name, password, and confirm password, and add face and fingerprint.

Figure 4-11 Add enforcer

Add

Enforcer Dept

Enforcer No

111

Enforcer Name

fr

Password

••••

Confirm Password

Password must be 8 to 32 characters, including at least two of the following categories: numbers, uppercase letters, lowercase letters and special characters (Characters like ' " ; : & cannot be included in).

Face

+ Add

Fingerprint

+ Add

OK

Back

Searching for Enforcer

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

Figure 4-12 Search for enforcer

ID	Name	Fingerprint/Face	Person	Dept	Modify	Delete	Device
1	lsc						
2	lsc2						

4.1.4.1.3 Resetting Password

Background Information

Enable the function, and you can reset password by taping on the login screen.

Procedure

- Step 1 Select **Setting** > **Account** > **Password Reset**, and 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 questions after successful setting, tap **Reset** first.
- Step 3 Tap **Apply**.

Figure 4-13 Reset password

The screenshot shows a web interface for configuring password reset. On the left is a sidebar with a menu containing 'User', 'Enforcer', and 'Password Reset' (which is highlighted). The main content area is titled 'Password Reset' and contains the following elements:

- An 'Enable' toggle switch, which is currently turned on.
- A 'Reserved Email' text input field.
- A 'Security Question' section with a message: 'Set successfully. Please reset first if you need to modify securi' followed by a 'Reset' button.
- Three security questions, each with a dropdown menu and a corresponding answer text input field:
 - Question 1: 'What is your favorite children's book?' (dropdown) and answer field.
 - Question 2: 'What was the first name of your first boss?' (dropdown) and answer field.
 - Question 3: 'What is the name of your favorite fruit?' (dropdown) and answer field.
- At the bottom right, there are 'Apply' and 'Back' buttons.

4.1.4.2 Network Management

4.1.4.2.1 TCP/IP

Background Information

You can configure IP address and 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.

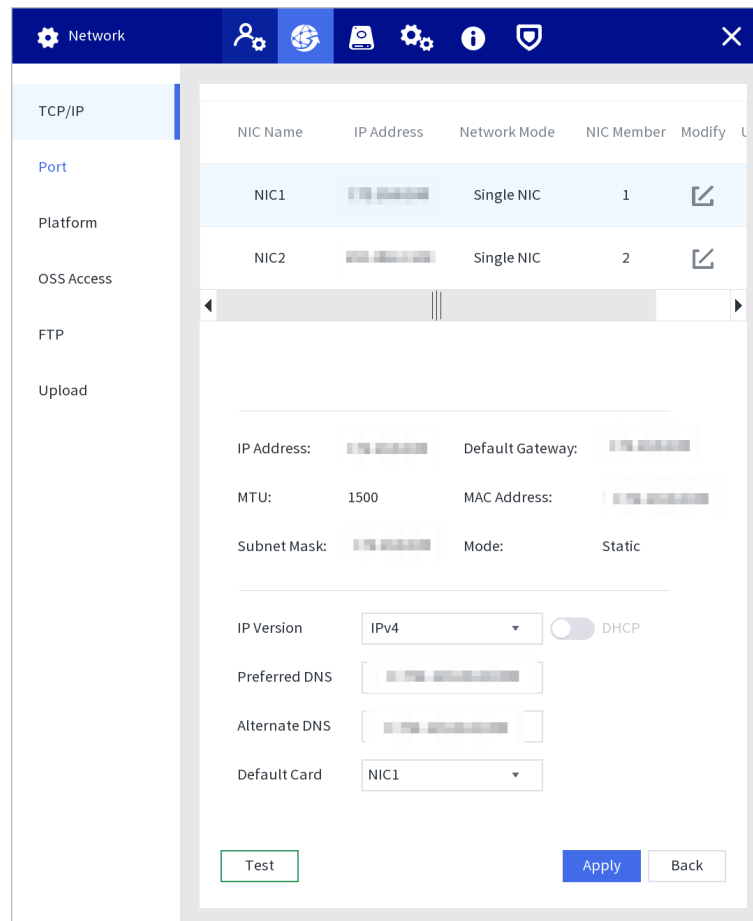
Procedure

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

Step 2 Configure Ethernet card parameters.

1. Tap  of the corresponding Ethernet card.
2. Configure Ethernet card parameters.

Figure 4-14 IP configuration



Step 3 Tap **Apply**.

4.1.4.2.2 Port

Background Information

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 4-15 Configure port parameters

The screenshot shows a configuration window titled 'Network' with a sidebar on the left containing options: TCP/IP, Port (selected), Platform, OSS Access, FTP, and Upload. The main area displays the following parameters:

Parameter	Value	Range
Max Connection	128	(0 - 128)
TCP Port	37777	(1025 - 65535)
UDP Port	37778	(1025 - 65535)
HTTP Port	80	(1 - 65535)
HTTPS Port	443	(1 - 65535)
NTP Server Port	123	(1 - 65535)

At the bottom right, there are 'Apply' and 'Back' buttons.

Table 4-2 Port parameters description

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.
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 Tap **Apply**.

4.1.4.2.3 Platform

Set up relevant functions for the interaction between the platforms.

Register

Background Information

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.

Prerequisites

- 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 > Register**.
- Step 2** Tap  to enable the function.
- Step 3** Configure the parameters.

Figure 4-16 Register

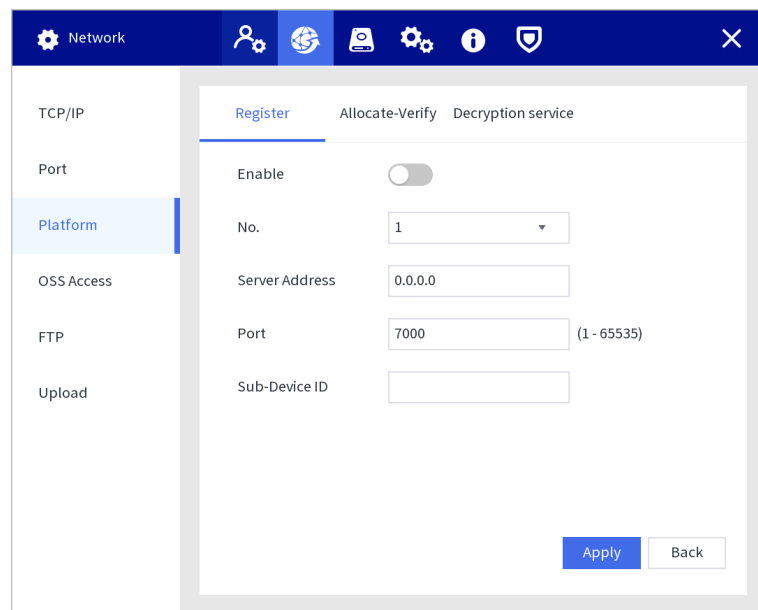


Table 4-3 Register parameters

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.
Sub-Device ID	This ID is allocated by the server and used for the Station.

- Step 4** Tap **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 4-17 Configure the allocate-verify function

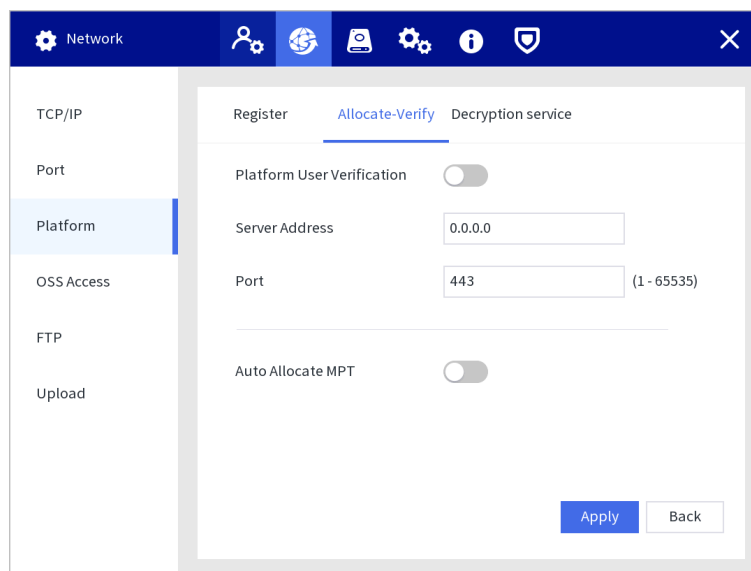


Table 4-4 Allocate-verify parameter description

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.
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, tap **Put In** to get in the idle position; when disconnecting the MPT, tap **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.

4.1.4.2.4 OSS Access

Background Information

Set up OSS access parameters to connect the device to the platform and enable data transmission with the platform.

Procedure

Step 1 Select **Setting** > **Network** > **OSS Access**.

Step 2 Enable the function of OSS access and configure the parameters.

Figure 4-18 OSS access

Table 4-5 OSS access

Parameter	Description
Server Address	Platform registration address.
Port	Platform registration port.

Parameter	Description
Username	Platform login username.
Password	Platform login password.
Device No.	Device number must match the one used when adding the device to the platform.

Step 3 Enable the function of upload and configure the parameters.

Table 4-6 Upload

Parameter	Description
Port	It is 50000 by default.
Protocol	Supports the selection of HTTP and HTTPS.  HTTPS is a secure encrypted transmission protocol.

4.1.4.2.5 FTP Setting

Background Information

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

Prerequisites

You have 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 parameters.



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

Figure 4-19 FTP setting

Table 4-7 FTP parameters

Parameter	Description
Server Address	The IP address of the FTP 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. - 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 Tap **Apply**.

4.1.4.2.6 Upload

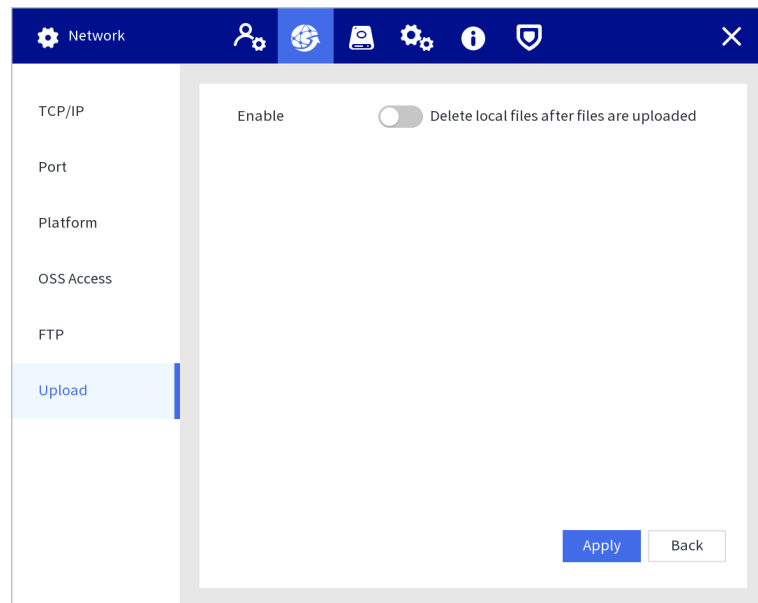
Enable the upload function; after files are uploaded to the platform or FTP, the corresponding files in the collection station will be deleted.

Procedure

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

Step 2 Click ☐ to enable the upload function.

Figure 4-20 Upload



Step 3 Click **Apply**.

4.1.4.3 Storage Management

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

4.1.4.3.1 Basic

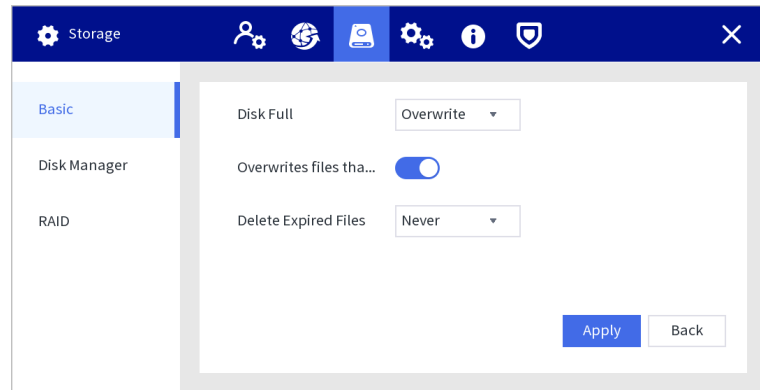
Procedure

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

Step 2 Configure parameters.

- **Disk Full** : Configure the settings for the situation that all the read/write disks are full, and there is no more free disk.
 - ◇ Select **Stop Record** to stop recording.
 - ◇ Select **Overwrite** to overwrite the recorded video files always from the earliest time.
- **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 that historical files will not be deleted. When **Custom** is selected, it allows for the configuration to delete files older than 1 to 255 days. Once this configuration is in place, it will actively delete historical data prior to that specified time.

Figure 4-21 Basic configuration



Step 3 Tap **Apply**.

4.1.4.3.2 Disk Manager

Background Information

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 Tap  to view the details.

Step 3 (Optional) Format an HDD.

1. Select an HDD and then tap **Format**.
2. Tap **OK**.
3. Enter the admin password and tap **OK**.

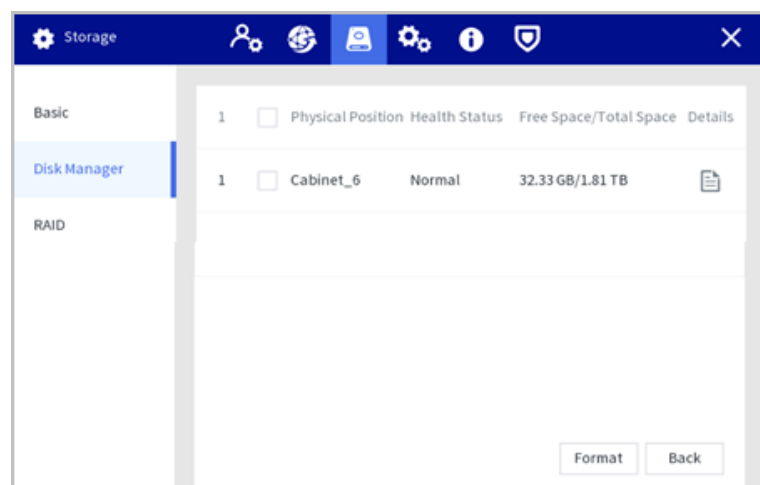
All data in the HDD is deleted.



DANGER

This operation will delete all data in the HDD. Proceed with caution.

Figure 4-22 Disk manager



4.1.4.3.3 RAID

RAID (redundant array of independent disks) is a data storage virtualization technology that combines multiple physical HDD components into a single logical unit for the purposes of data redundancy, performance improvement, or both.



- The Station supports RAID 0, RAID 1, RAID 5, RAID 10. For details, see #unique_52/unique_52_Connect_42 RAIDfulu. This section takes RAID 5 as an example.
- We recommend deploying RAID disks at the beginning of RAID configuration. Creating or deleting RAID will affect device data.

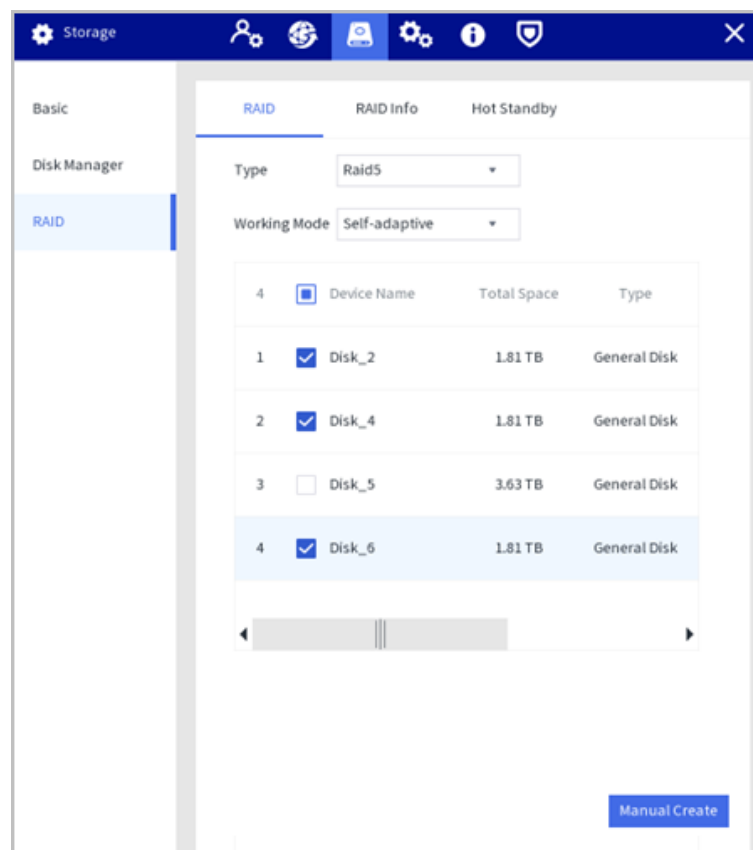
Configuring RAID

1. Step 1 Select **Setting** > **Storage** > **RAID** > **RAID**.
2. Select RAID type and working mode.

When you select RAID 5 in **Type**, you can set the work mode.

- **Self-adaptive** : The system can automatically adjust RAID synchronization speed according to current business load. When there is no external business running, the synchronization is performed at high speed. When there is external business running, the synchronization is performed at low speed.
- **Sync first** : Resources are allocated to RAID synchronization first.
- **Business first** : Resources are allocated to business first.
- **Load-balance** : Resources are allocated to business and RAID synchronization equally.

Figure 4-23 RAID



3. Select the disk where you want to create RAID.

- 4. Tap **Manual Create**.
- 5. Tap **Confirm**.

After authentication, RAID is created successfully, and the information of the new RAID is displayed.

Figure 4-24 Create RAID successfully

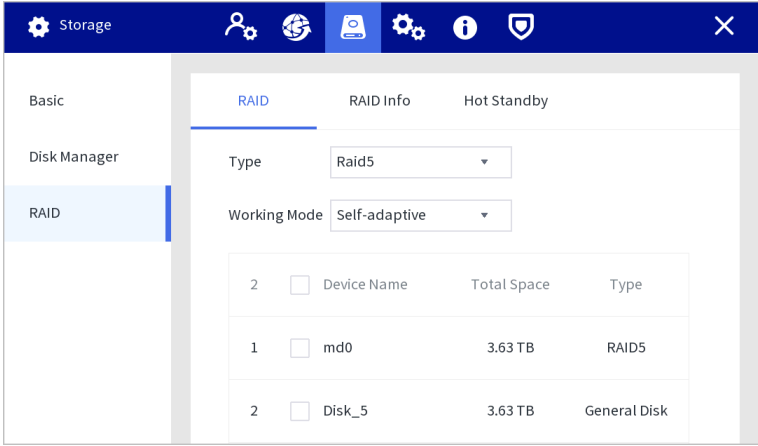


Figure 4-25 Display in disk manager RAID is created (1)

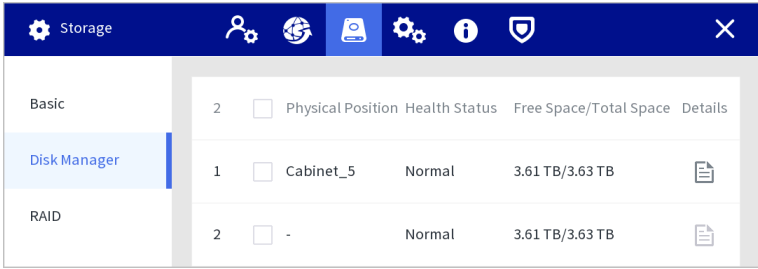
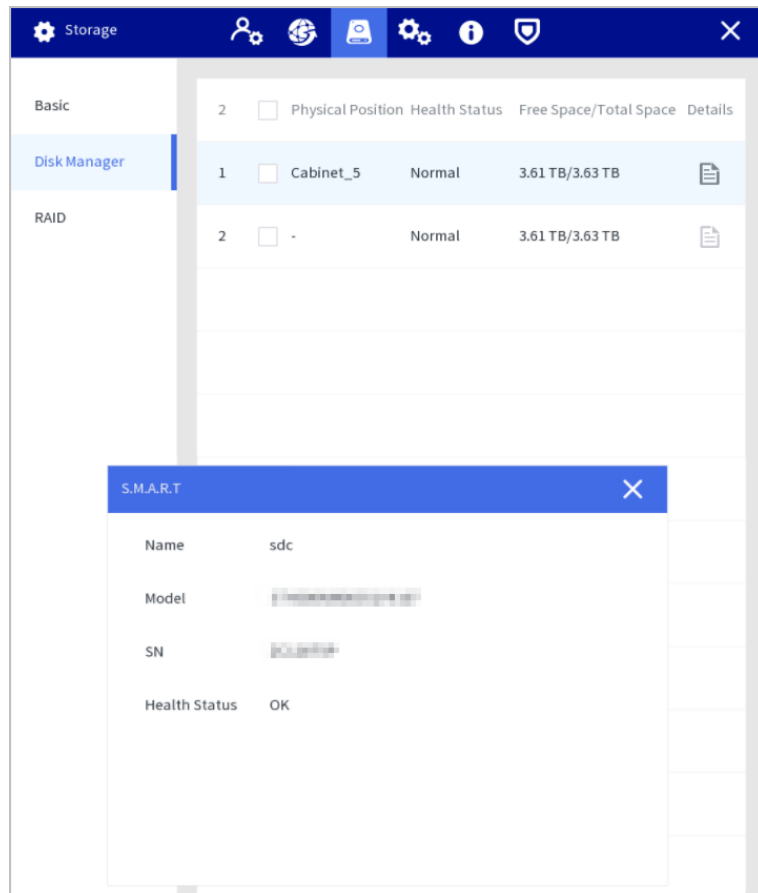


Figure 4-26 Display in disk manager RAID is created (2)



RAID Information

You can view RAID information including device name, total space, and type.

Select **Setting** > **Storage** > **RAID** > **RAID Info**, and then tap the RAID to see the details.

Figure 4-27 RAID information

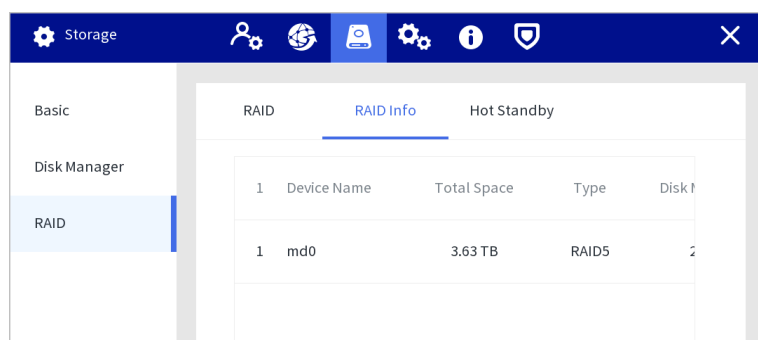


Figure 4-28 Details

Details

RAID Name

md0

Type

RAID5

Space Info

3.61 TB / 3.63 TB

Working Mode

Self-adaptive

Status

Active,Degraded,Recovering

Sync Progress

0.100%

Sync Speed

7.146 MBps

Sync End Time

3	Disk Members	Physical Position	Space Info	Status	Delete
1	/dev/sda	SATA-2	1.81 TB	Sync	
2	/dev/sdd	SATA-6	1.81 TB	Rebuilding	
3	/dev/sdb	SATA-4	1.81 TB	Sync	

OK

Cancel

Hot Standby

When an HDD of the RAID group has a problem, the hot spare HDD can replace the malfunctioning HDD. There is no risk of data loss and it can guarantee storage system reliability.

1. Select **Setting > Storage > RAID > Hot Standby**.
2. Select device type and the RAID group that needs to add hot spare HDD.
 - Private hot spare: Select a RAID group to be added, and then the HDD will be added to the corresponding RAID group, and used as a hot spare HDD for the RAID.
 - Global hot standby: It is a hot spare HDD for all RAID groups rather than a specific RAID group.

Figure 4-29 Private hot spare

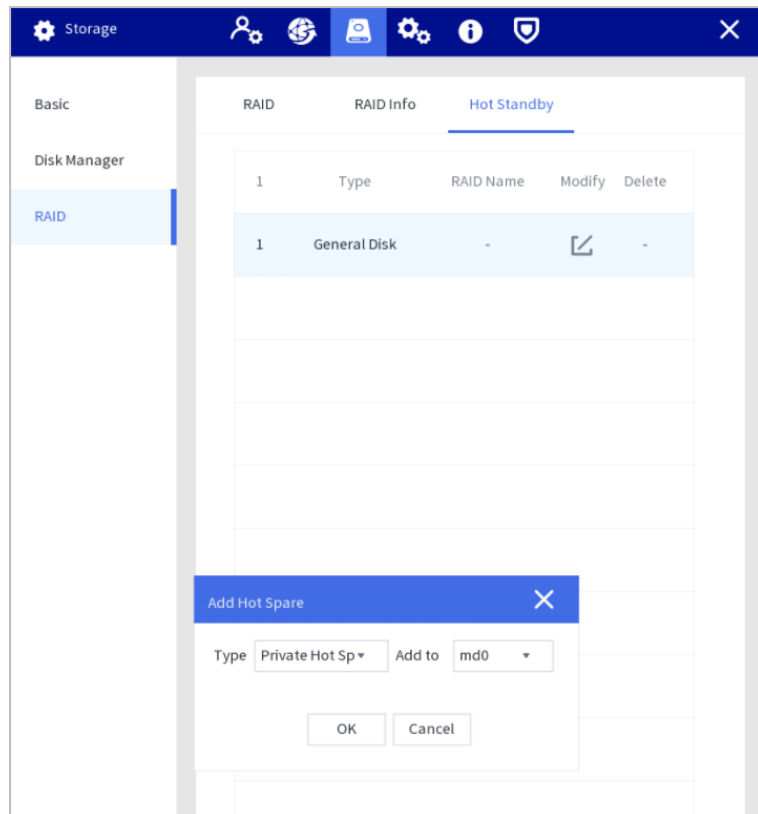
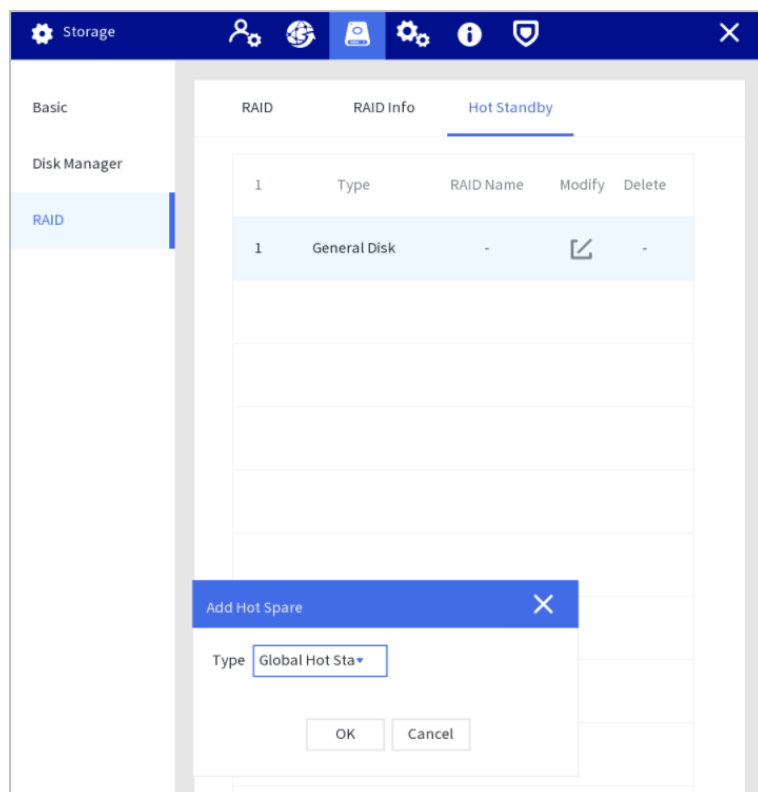


Figure 4-30 Global hot standby



3. Tap **OK**.

After authentication, the hot standby is created successfully.

Figure 4-31 Global hot standby

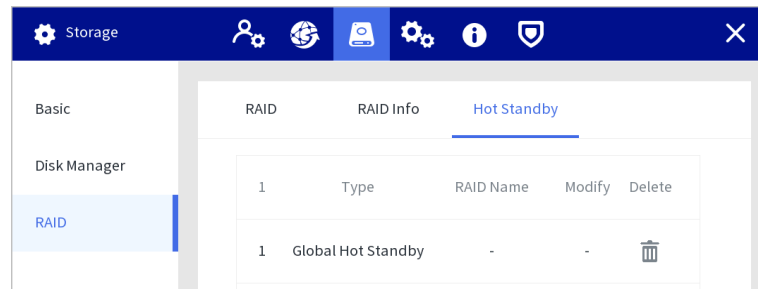
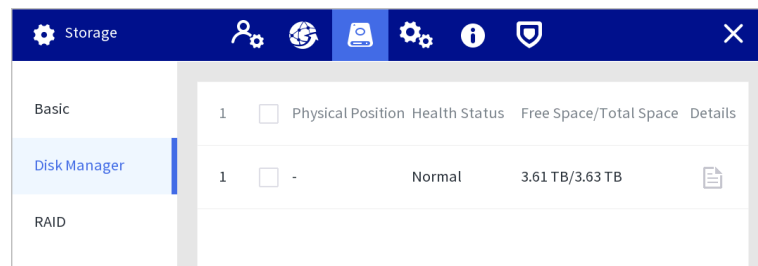


Figure 4-32 Display in disk manager after hot standby is created



4.1.4.4 System Management

4.1.4.4.1 Basic Setting

You can set the screen off time, logout time, video standard, and decide whether to trigger alarm when network disconnection occurs.

Figure 4-33 Basic setting

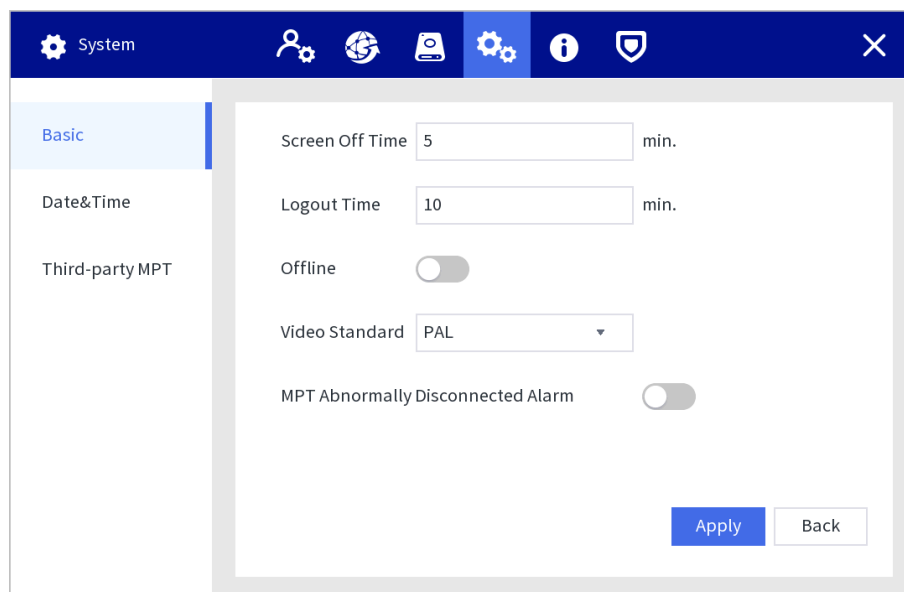


Table 4-8 Date and time parameters

Parameter	Description
Screen Off Time	Set the screen off time. When you do not operate the Station within the defined time, the screen will be off. It ranges from 0–60 minutes, and 0 means the screen will always be on. To extend service life of the LCD screen, we recommend you not to set the time as 0 minutes.
Logout Time	Set auto 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. 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 will be triggered when network disconnection occurs on any Ethernet port.
Video Standard	Select video standard from PAL and NTSC . Restart the Station after switching the video standard to make the configuration take effect.
MPT Abnormally Disconnected Alarm	Enable the alarm function. If the recorder is pulled out abnormally or other situations occur, an alarm will be triggered.

4.1.4.4.2 Date and Time

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

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. You can set the time manually or through NTP.

Figure 4-34 Date and time

System Time: 2021-02-27 20:21:15 [Save]

Time Zone: (UTC+08:00) Beijing, C

Date Format: YYYY MM DD

Date Separator: -

Time Format: 24-Hour

DST: ☐

Type: ☒ Date ☐ Week

Start Time: Jan 1 00:00

End Time: Jan 2 00:00

NTP: ☐

Server Address: time.windows.com [Manual Update]

Port: 123 (1-65535)

Interval: 60 min. (0-65535)

2. Set the time manually.

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

Table 4-9 Date and time parameters

Parameter	Description
System Time	Set the device system date and time. Tap 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 .

Parameter	Description
DST	When you enable DST, 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.

3. Enable NTP.

Enable NTP, and enter the server address, 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.

4. Tap **Apply**.

4.1.4.5 Operation & Maintenance Management

4.1.4.5.1 System Information

You can view the device model, hardware version, system version, and web version.

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

Figure 4-35 Version information

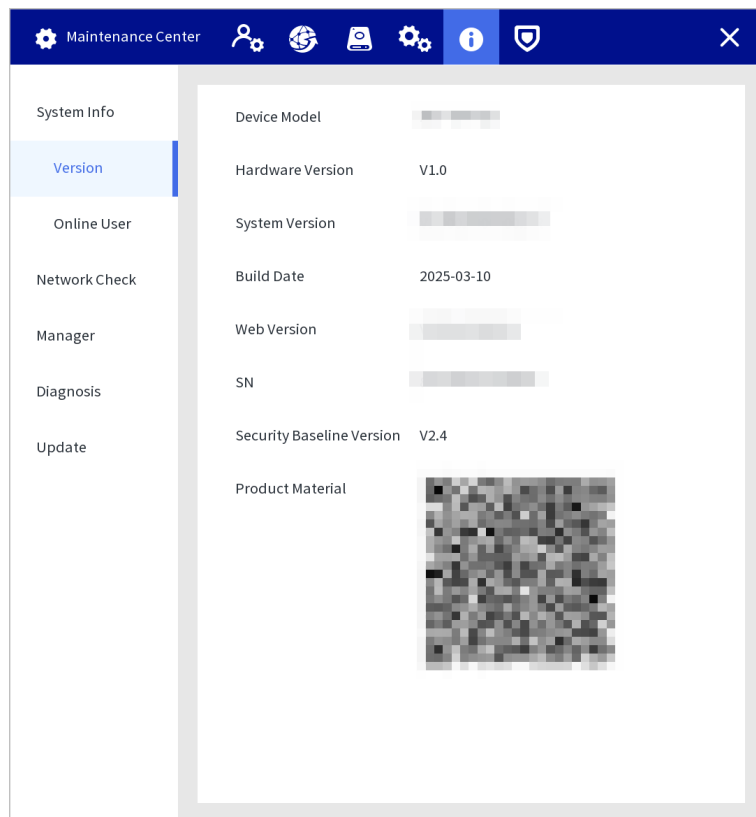
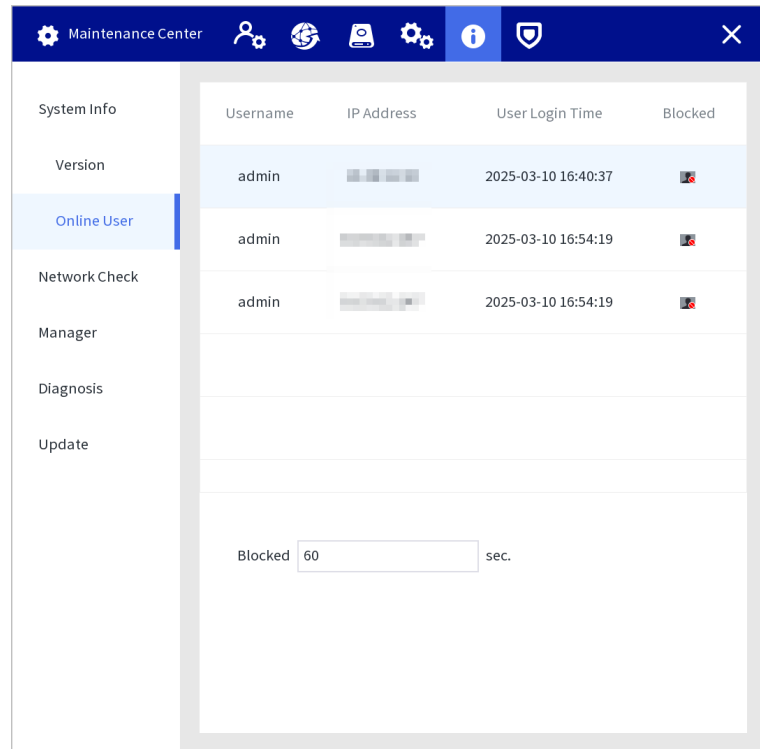


Figure 4-36 Online user information



The screenshot shows a web interface titled 'Maintenance Center' with a sidebar menu and a main content area. The sidebar menu includes 'System Info', 'Version', 'Online User' (highlighted), 'Network Check', 'Manager', 'Diagnosis', and 'Update'. The main content area displays a table of online users with columns for Username, IP Address, User Login Time, and Blocked. Below the table is a 'Blocked' section with a text input field containing '60' and a label 'sec.'.

Username	IP Address	User Login Time	Blocked
admin	[REDACTED]	2025-03-10 16:40:37	
admin	[REDACTED]	2025-03-10 16:54:19	
admin	[REDACTED]	2025-03-10 16:54:19	

Blocked sec.

4.1.4.5.2 Network Check

Background Information

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



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

Procedure

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

Figure 4-37 Network check

Name	IP	Packet Sniffer Size	Packet Sniffer Backup
LAN1	[Redacted]	0KB	[Download Icon]
Loopback	[Redacted]	0KB	[Download Icon]

Step 2 Enter the destination IP and click **Test** to check the connectivity between the current network and the destination IP.

The results will be displayed in the test results.

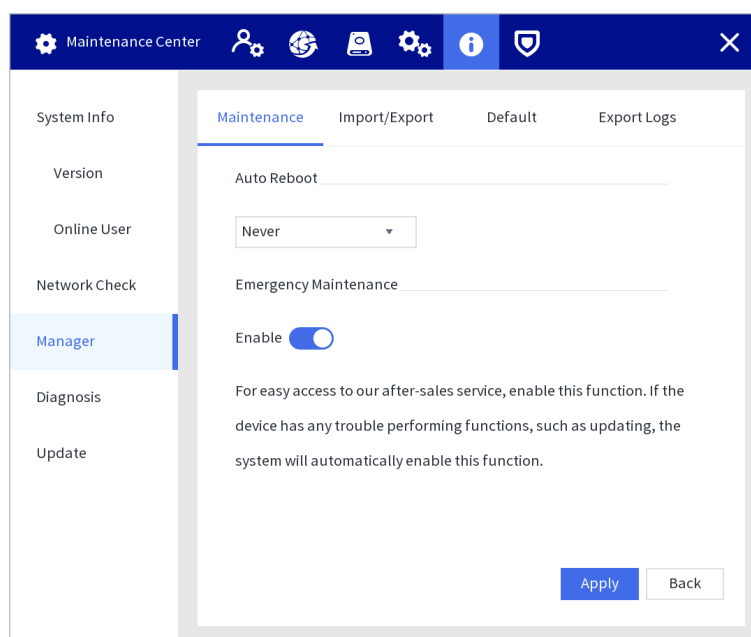
Step 3 Connect a USB drive to the device, click **Browse** to select the packet sniffer backup storage path, and then click **Start** to save the corresponding packet sniffer to the specified storage path.

4.1.4.5.3 Device Maintenance

Device Maintenance

1. Select **Setting** > **Maintenance Center** > **Manager** > **Maintenance**, and then set the auto reboot frequency.

Figure 4-38 Device maintenance



2. 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.

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 4-39 Export configuration

The screenshot shows the 'Maintenance Center' application window. The left sidebar contains 'System Info', 'Version', 'Online User', 'Network Check', 'Manager' (highlighted), 'Diagnosis', and 'Update'. The main panel has tabs for 'Maintenance', 'Import/Export' (selected), 'Default', and 'Export Logs'. Under the 'Import/Export' tab, the 'Operation Type' is set to 'Export'. 'File Type' is 'HDD Database'. 'Path' and 'Password' are empty text boxes with 'Browse' and an eye icon respectively. A 'Start' button is present. Below, 'Auto Backup to Disk' is a toggle switch. 'Latest Version(Disk)' and 'Latest Version(User)' are both 'Null' with 'Import' buttons. A note at the bottom states: 'The collection status information of all slots will be reset, during process.'

Figure 4-40 Import configuration

This screenshot is identical to Figure 4-39, but the 'Operation Type' dropdown is set to 'Import'. All other elements, including the sidebar, tabs, text boxes, buttons, and the bottom note, remain the same.

Default

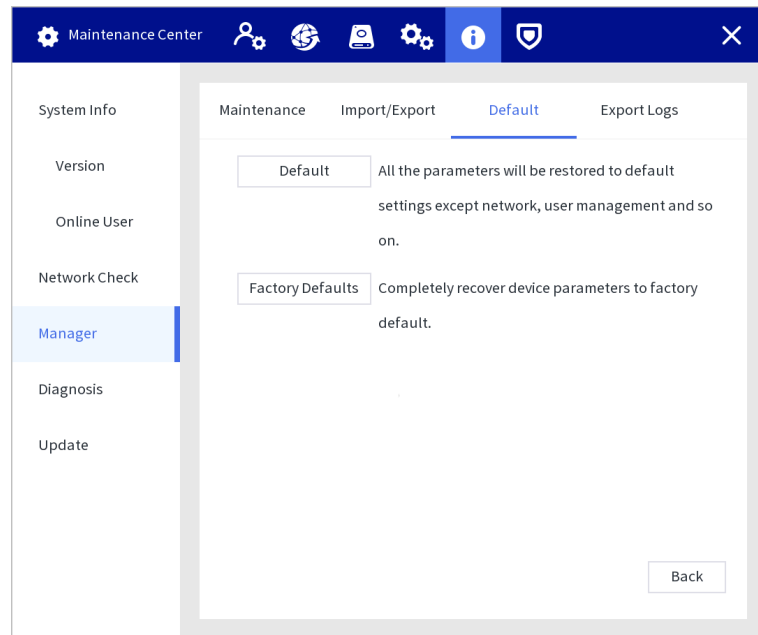
When the system runs slowly and has configuration errors, try to solve the problems by restoring the default settings.



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 4-41 Default



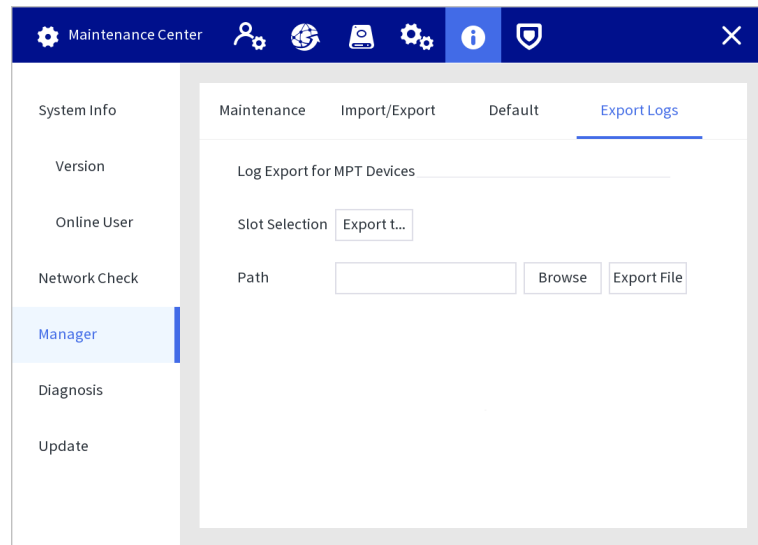
- Default: Tap **Default**, and the parameters such as except network, user management will be restored to default setting.
- Factory default: Tap **Factory Defaults**, and the tip dialog is displayed. Tap **OK**. All parameters will be restored to the factory default settings.

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 USB drive** to select the slot.

Figure 4-42 Export logs

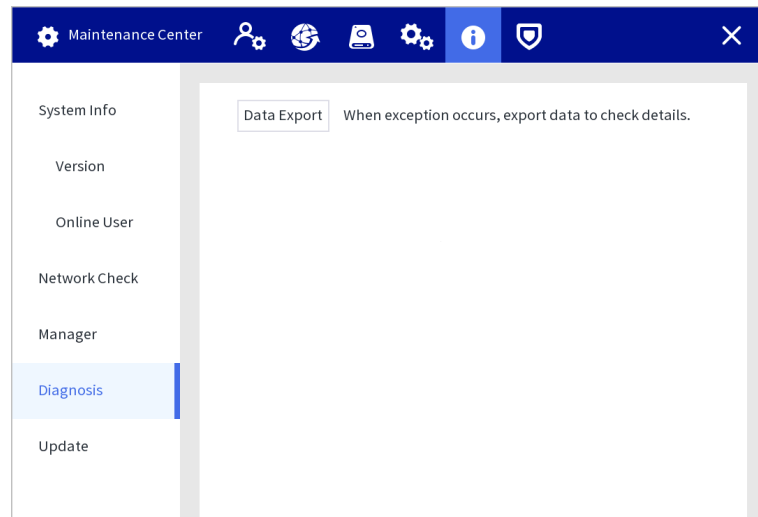


3. Click **Browse**, and then select the MPT and the path.
4. Click **Export File**.

4.1.4.5.4 Diagnosis

Click **Data Export** to export data of the device health, such as emmc lifespan for issue verification.

Figure 4-43 Diagnosis

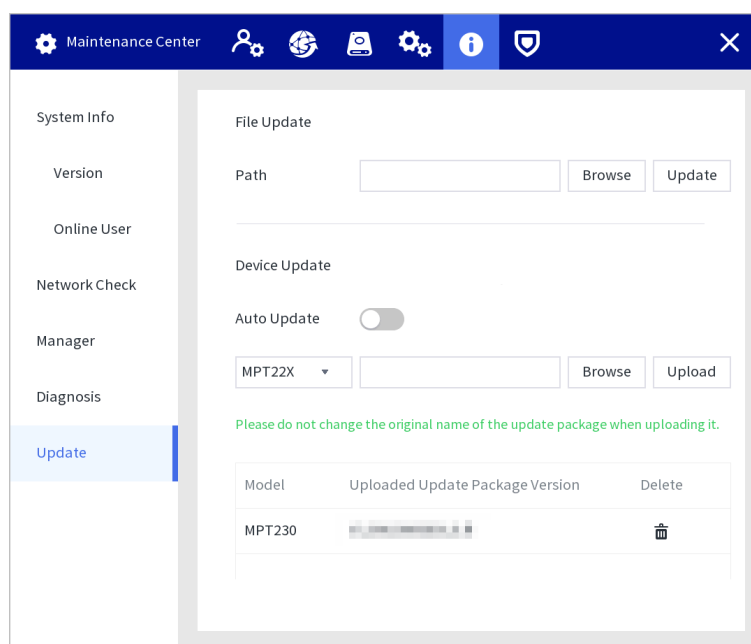


4.1.4.5.5 Update

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 4-44 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.

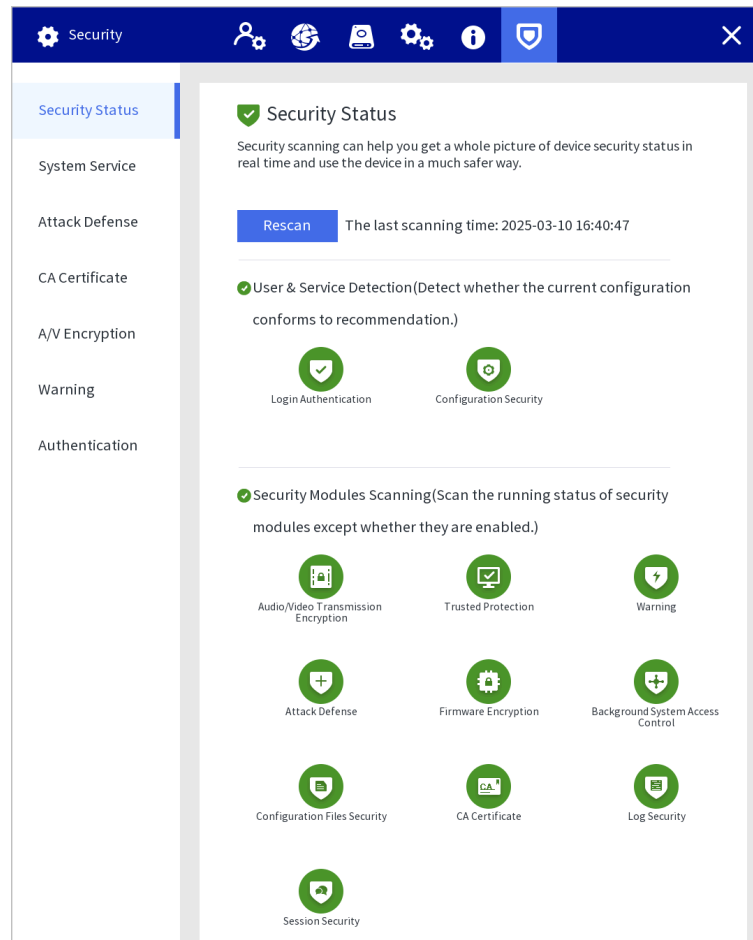
4.1.4.6 Security

4.1.4.6.1 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.
 1. Select **Setting** > **Security** > **Security Status**.
 2. Tap **Rescan** to scan the security status of the Station.

Figure 4-45 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.

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

- Tap **Ignore** to ignore the exception, and it will not be scanned in next scanning.



Tap **Rejoin Detection**, and the exception will be scanned in next scanning.

- Tap **Optimize**, and the corresponding screen is displayed, and you can edit the configuration to clear the exception.

4.1.4.6.2 System Service

Basic Services

1. Select **Setting > Security > System Service > Basic Services**.
2. Configure parameters.

Figure 4-46 Basic services

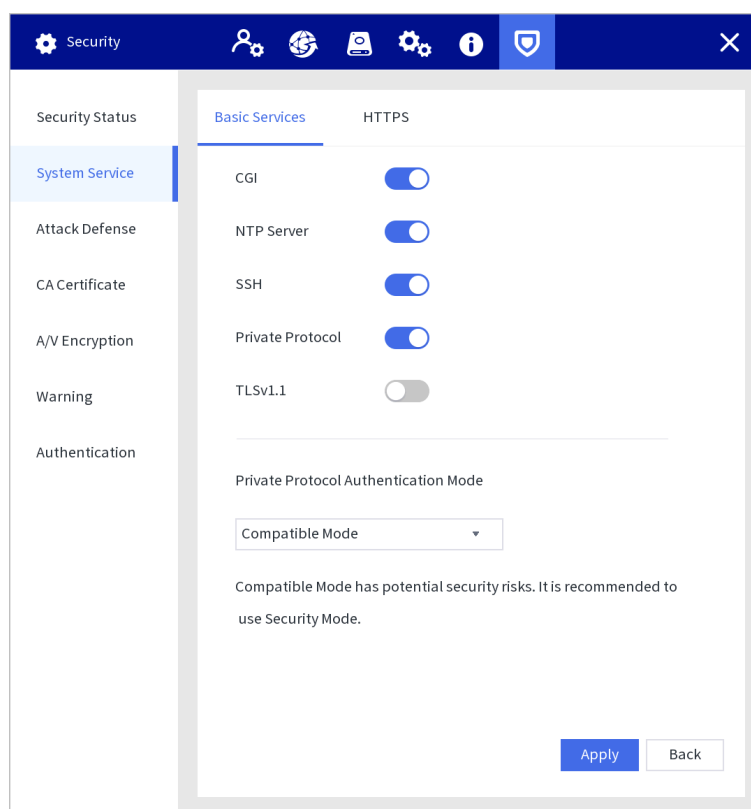


Table 4-10 Description of basic service parameters

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. It is enabled by default.
Private Protocol	Enabled by default; disabling it will prevent private protocol communication, ensuring secure management.
TLSv1.1	Encryption protocol; once enabled, lower versions below 1.1 will no longer be supported.
Private Protocol Authentication Mode	Select private protocol authentication mode to guarantee the device security when login. Security Mode is recommended.

3. Click **Apply**.

HTTPS

Through creating server certificate, the computer can log in to the device by HTTPS to ensure the security of communication data and guard the user information and device security with stable technology measure.



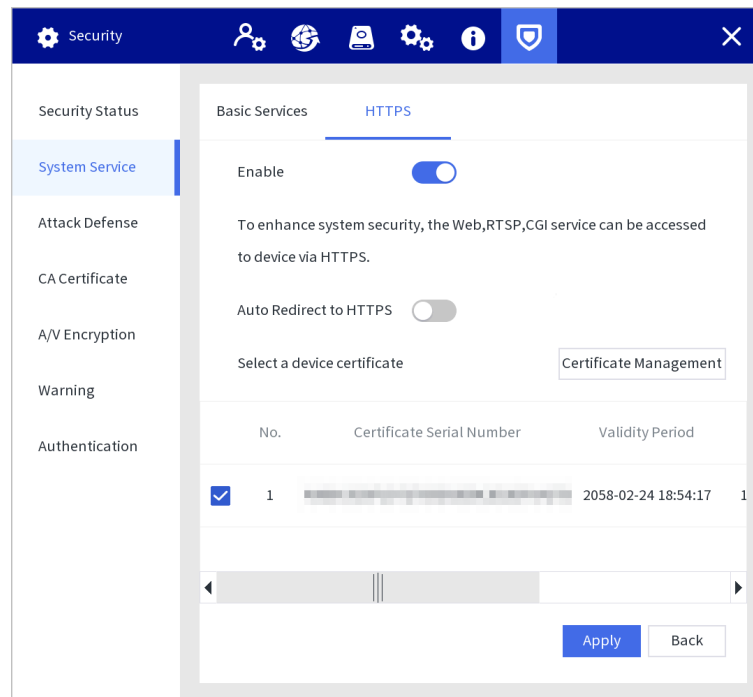
We recommend you use HTTPS service. If the service is disabled, there might be risk of data leakage.

1. Select **Setting** > **Security** > **System Service** > **Basic Services** > **HTTPS**.
2. Enable HTTPS, and then select the certification.



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

Figure 4-47 HTTPS



3. (Optional) Tap ☐ next to **Auto Redirect to HTTPS** to enable the automatic redirection to HTTPS function.
4. Tap **Apply**.

Results

Open the browser, enter *https://device IP:port*, and then press the Enter key.



Port refers to HTTPS port number. If the HTTPS port is 443, just enter *https://device IP*.

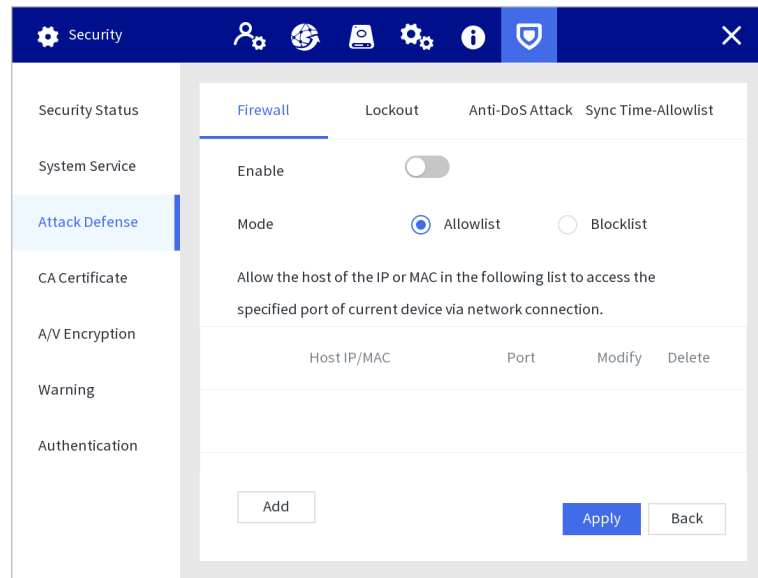
4.1.4.6.3 Attack Defense

Firewall

Configure firewall to limit access to the Station.

1. Select **Setting** > **Security** > **Attack Defense** > **Firewall**.
2. Enable the firewall function.

Figure 4-48 Firewall



3. Select the access mode.

Allowlist and Blocklist cannot be enabled at same time.

- Allowlist: Only when the IP/MAC of your computer in the allowlist, can you access the Station.
- Blocklist: When the IP/MAC of your computer is in the blocklist, you cannot access the Station.

4. Add the host IP/MAC address to allowlist or blocklist.

- a. Tap **Add**.
- b. Enter the information of IP host.

Figure 4-49 Add allowlist

- c. Tap **Apply**.

Account Lockout

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

1. Select **Setting > Security > Attack Defense > Lockout**.
2. Configure parameters.
 - **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 4-50 Account lock

The screenshot shows the 'Lockout' configuration page within the 'Attack Defense' section of the 'Security' settings. The interface has a dark blue header with icons for various security features. A left sidebar lists navigation options: Security Status, System Service, Attack Defense (highlighted), CA Certificate, A/V Encryption, Warning, and Authentication. The main content area is titled 'Lockout' and contains three sections: Password Login, Face Login, and Fingerprint Login. Each section provides a description of the lockout policy and input fields for 'Login Attempt' and 'Lock Time'. At the bottom right, there are 'Apply' and 'Back' buttons.

Section	Login Attempt	Lock Time
Password Login	5	5 min.
Face Login	10	5 min.
Fingerprint Login	5	5 min.

3. Tap **Apply**.

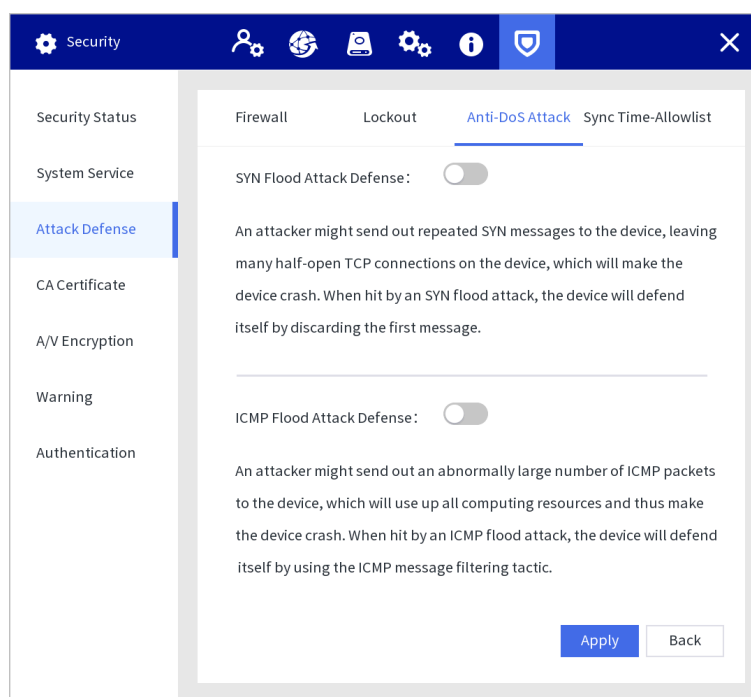
Anti-DoS Attack

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

1. Select **Setting > Security > Attack Defense > Anti-DoS Attack**.

2. You can enable SYN Flood Attack Defense and ICMP Flood Attack Defense to defend the device against Dos attack.

Figure 4-51 Anti-DoS attack



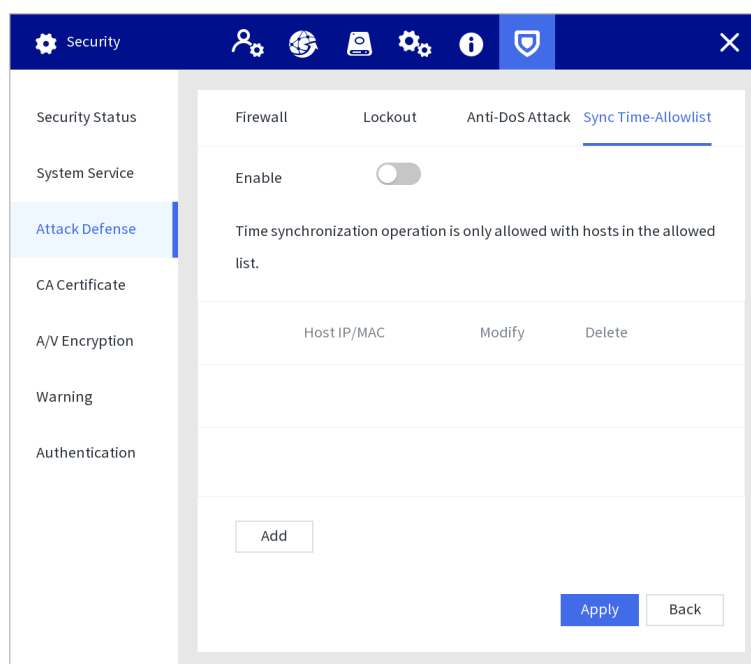
3. Tap **Apply**.

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. Select **Setting > Security > Attack Defense > Sync Time-Allowlist**.
2. Enable the sync time-allowlist function.

Figure 4-52 Sync time-allowlist



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

Figure 4-53 Add IP address

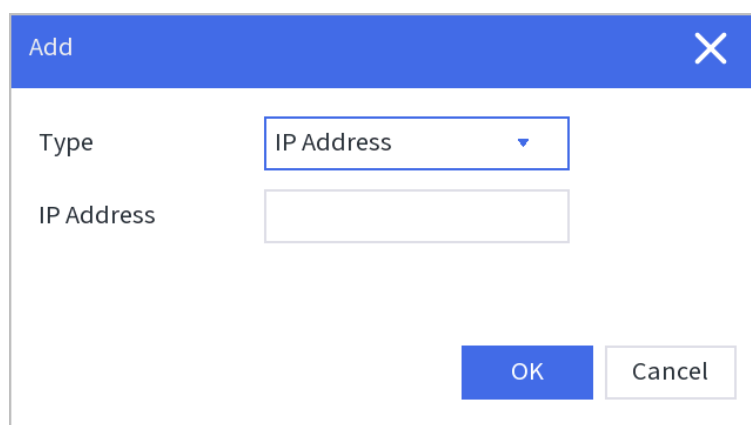
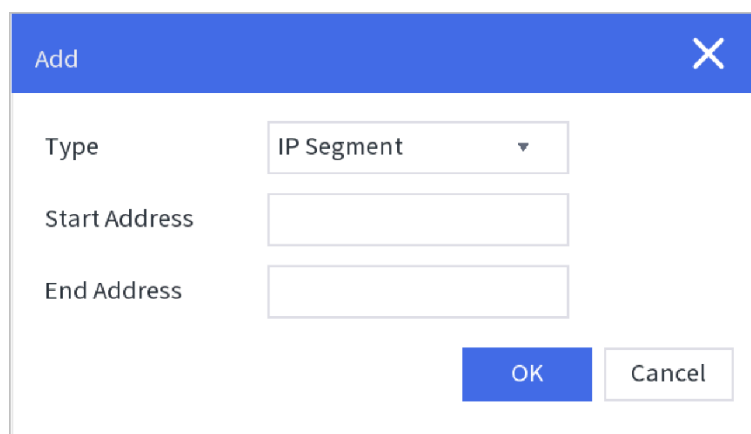


Figure 4-54 IP segment



4. Tap **Apply**.

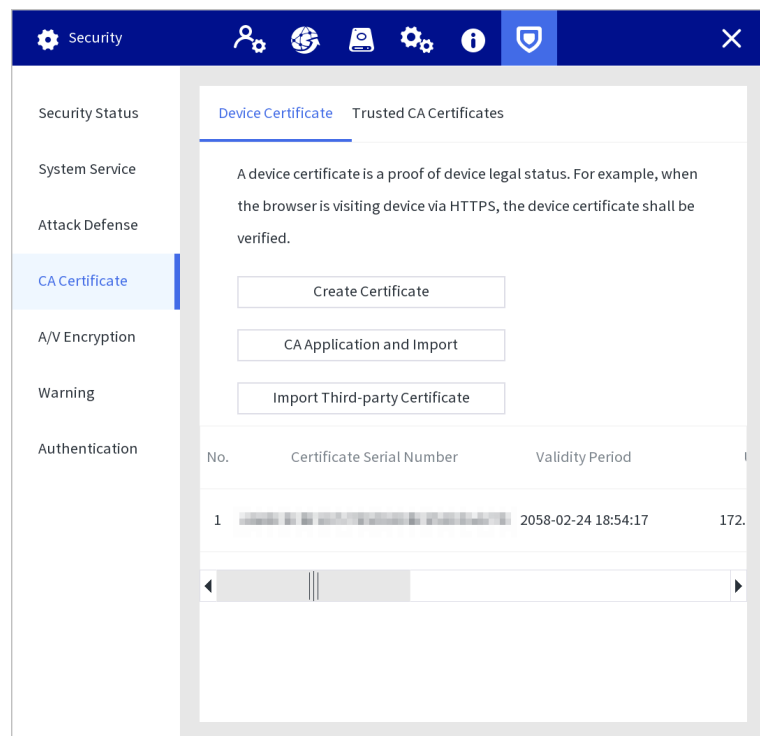
4.1.4.6.4 CA Certificate

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

Creating certificate

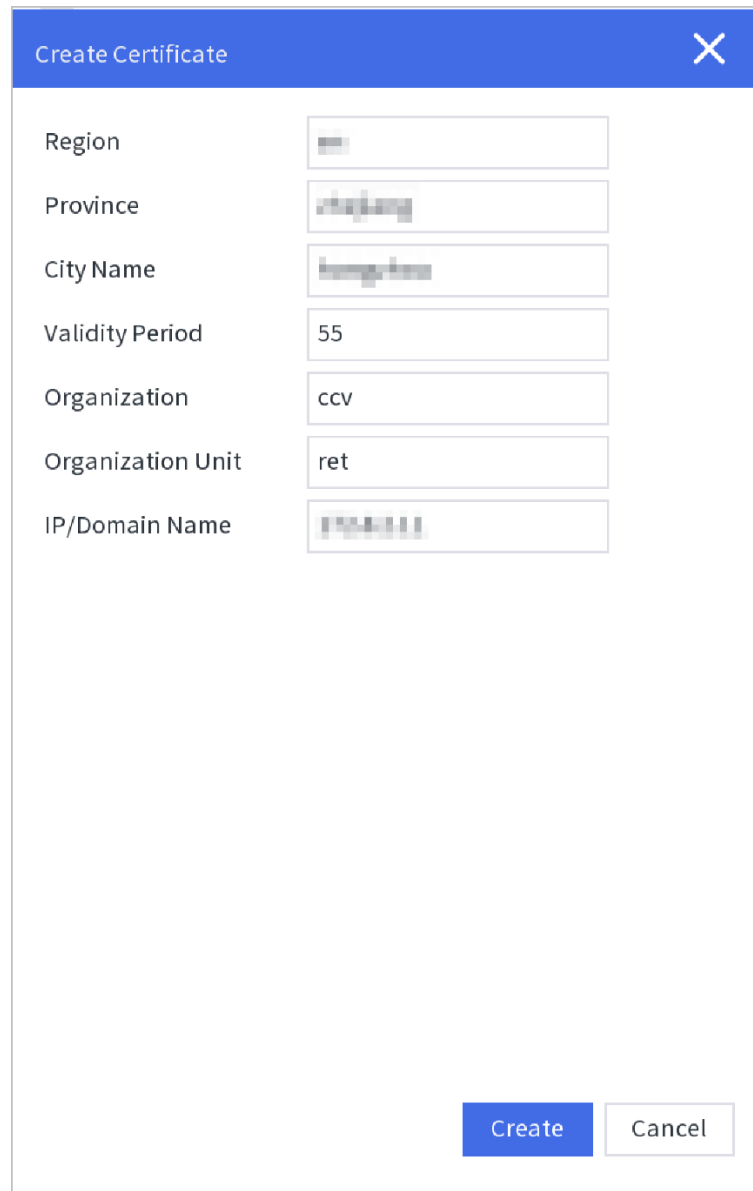
1. Select **Setting** > **Security** > **CA Certificate** > **Device Certificate**.
2. Tap **Create Certificate**.

Figure 4-55 Device certificate



3. Enter the certificate information.

Figure 4-56 Create certificate



The image shows a 'Create Certificate' dialog box with a blue header bar containing a close button (X). The dialog contains seven input fields for certificate information: Region, Province, City Name, Validity Period, Organization, Organization Unit, and IP/Domain Name. At the bottom right, there are two buttons: 'Create' (blue) and 'Cancel' (white with a blue border).

Field	Value
Region	
Province	zhongguo
City Name	hangzhou
Validity Period	55
Organization	ccv
Organization Unit	ret
IP/Domain Name	192.168.1.1

4. Tap **Create**.

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

Applying for and Importing CA Certificate

1. Select **Setting > Security > CA Certificate > Device Certificate**.
2. Tap **CA Application and Import**.
3. Enter the certificate information, and tap **Create** to save the certificate to an external device.

Figure 4-57 Apply for and importing CA certificate

CA Application and Import

Procedure:

Step 1: Select 'Create a Certificate Request' to generate a certificate request file.

Step 2: Submit the certificate request file to a third-party CA institution to apply for a certificate.

Step 3: Select 'Import a Certificate' and then import the CA certificate issued by the third-party institution.

Type **Create Certificate Request** Import Certificate

Region

Province

City Name

Validity Period

Organization

Organization Unit

IP/Domain Name

Create Cancel

4. Apply for the CA certificate from the third-party certificate authority.
5. Import CA certificate.
 - a. Save the CA certificate to a USB flash drive, and then insert the drive to the Station.
 - b. Tap **Import Certificate** on the **CA Application and Import** screen.
 - c. Import the certificate according to the screen instruction.

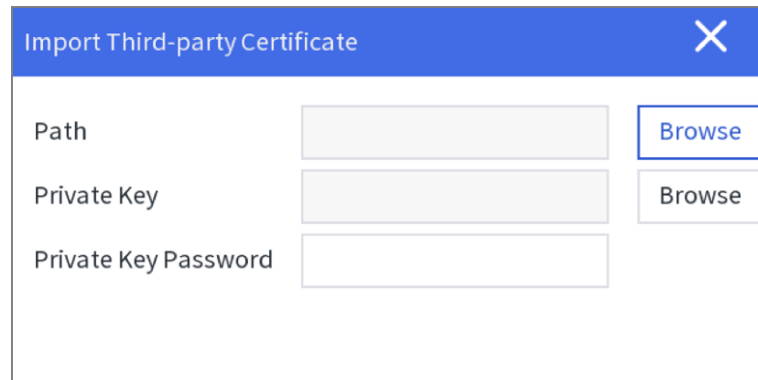
After the certificate is imported successfully, you can view the created certificate on the **Device Certificate** screen.

Importing Third-party Certificate

Save the third-party certificate to a USB flash drive, and then insert the drive to the Station.

1. Select **Setting > Security > CA Certificate > Device Certificate**.
2. Tap **Import Third-party Certificate**.
3. Select the certificate and private key file, and enter the private key password.

Figure 4-58 Import third-party certificate



4. Tap **Import**.

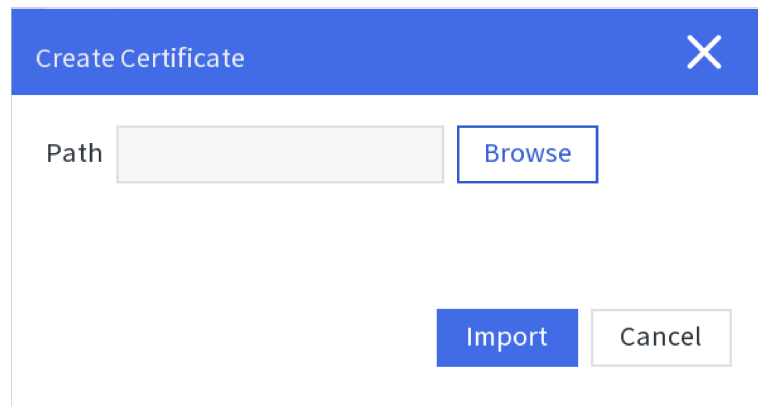
After the certificate is imported successfully, you can view the created certificate on the **Device Certificate** screen.

Installing Trusted CA 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.

1. Select **Setting** > **Security** > **CA Certificate** > **Trusted CA Certificate**.
2. Tap **Install Trust Certificate**.

Figure 4-59 Install trusted CA certificate



3. Tap **Browse** to select the certificate on the prompt screen, and then tap **Import**.

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

4.1.4.6.5 A/V Encryption

Background Information

The Station supports audio and video encryption during data transmission.



We recommended you 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 parameters.

Figure 4-60 A/V encryption

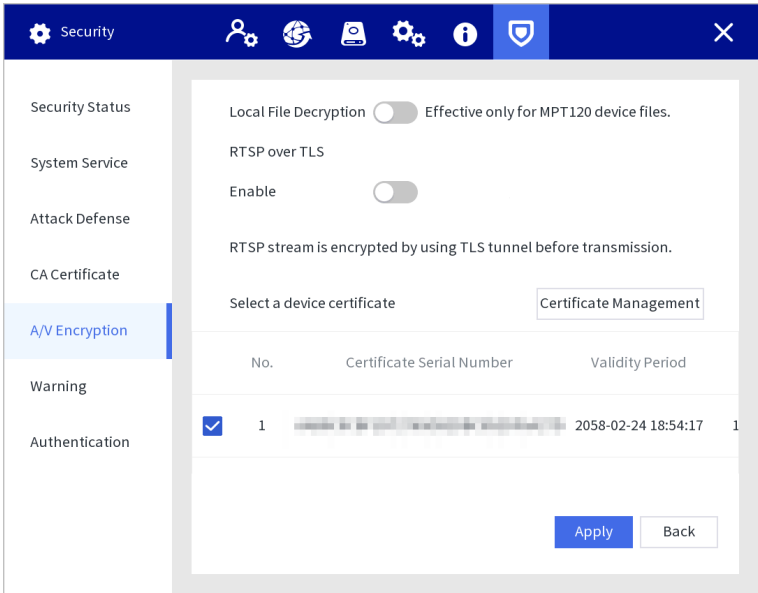


Table 4-11 Audio and video description

Encryption Type	Parameter	Description
Local file encryption	Enable	When you collect the encrypted files from the W1body camera, process the decryption first before collecting the data.
RTSP over TLS	Enable	Enables RTSP stream encryption by using TLS. Enable RTSP over TLS , 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

Tap **Apply**.

4.1.4.6.6 Security Warning

Security Exception

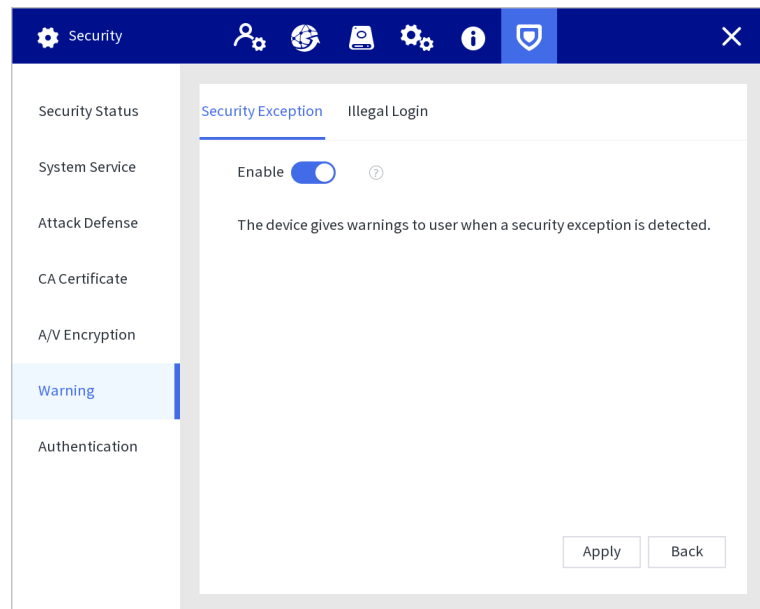
Immediately after detecting security abnormal behaviors, the Station sends a security warning to remind the user timely.

1. Select **Setting** > **Security** > **Warning** > **Security Exception**.
2. Enable security warning.



Tap  to view the details of the security exception event.

Figure 4-61 Security exception



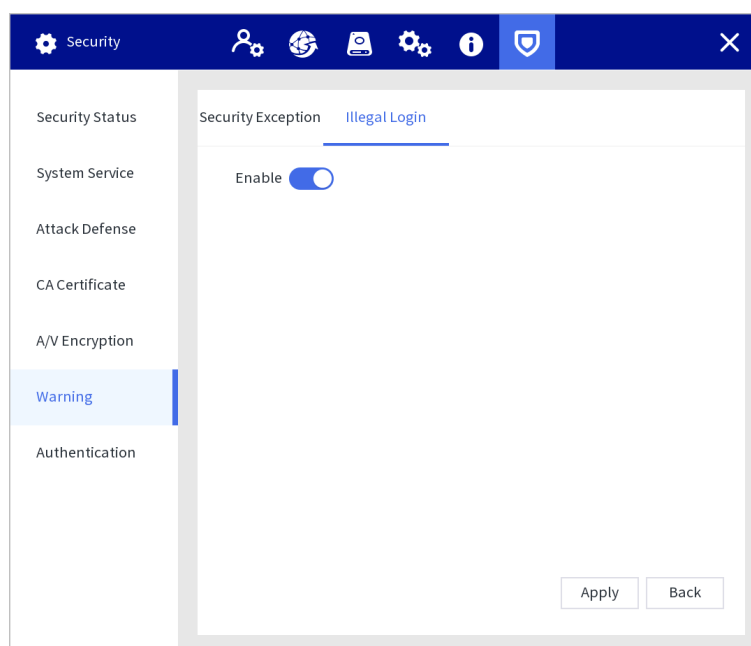
3. Tap **Apply**.

Illegal Login

Immediately after detecting invalid login, the device sends a security warning to remind the user timely.

1. Select **Setting** > **Security** > **Warning** > **Illegal Login**.
2. Enable illegal login warning.

Figure 4-62 Illegal login

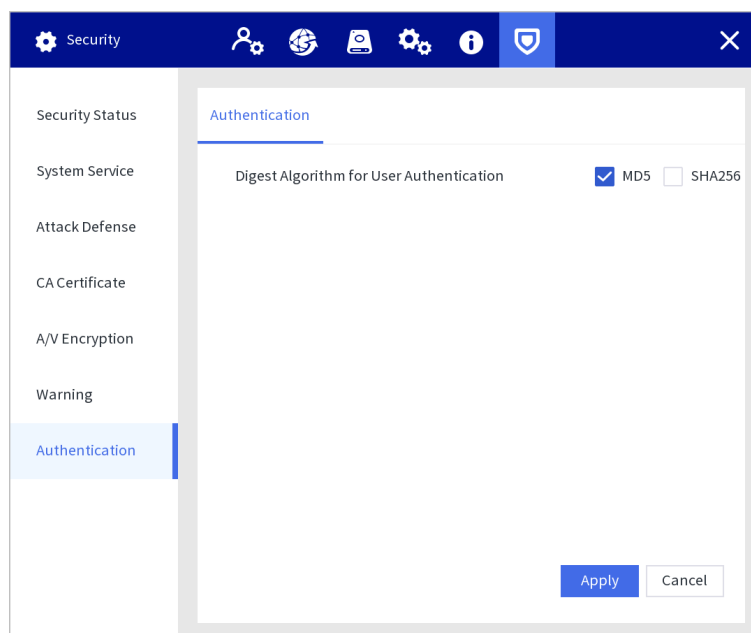


3. Tap **Apply**.

4.1.4.6.7 Security Authentication

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

Figure 4-63 Select digest algorithm for user authentication



4.1.5 Platform Configuration

Background Information

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

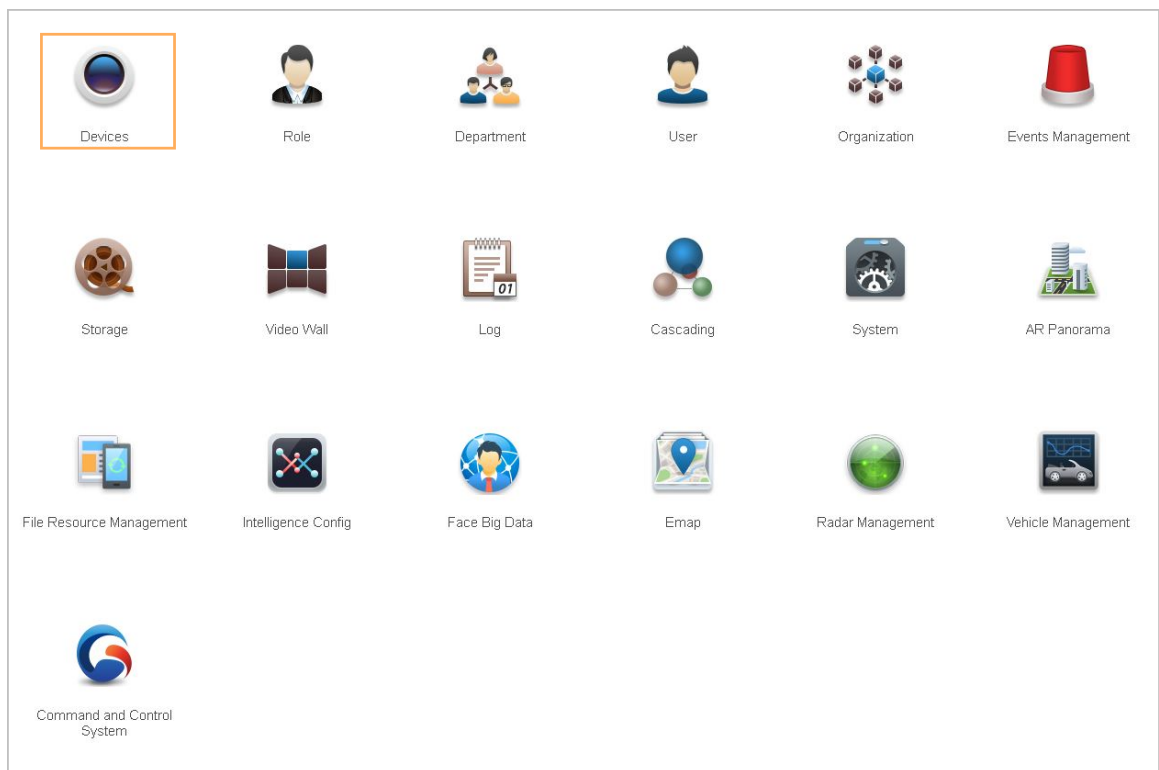


The following operations are for reference only. The actual operation might vary depending on the actual platform you are using.

Procedure

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

Figure 4-64 Home page



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

Figure 4-65 Login information

Table 4-12 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 .
Registration	When the Add Type is Auto Registration , enter the sub-device ID of the Station.
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	

Parameter	Description
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 defaultPaaS.

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

Figure 4-66 Device information

The screenshot shows a web-based configuration window titled "Add Devices" with a close button (X) in the top right corner. The window is divided into two tabs: "1. Login Info" and "2. Device Info", with the second tab being the active one. Below the tabs, there are four configuration fields:

- Device Name :** A text input field containing the value "caijizhan".
- Type :** A dropdown menu currently showing "Collection Station".
- Video Channel :** A dropdown menu currently showing "1".
- Alarm Input Channel :** A dropdown menu currently showing "0".

At the bottom of the dialog, there are three buttons: "Previous" (disabled), "Continue Add" (disabled), and "OK" (active).

Table 4-13 Device information parameters

Parameter	Description
Device Name	Customize 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**.

4.2 Web Configuration

4.2.1 Login

Background Information



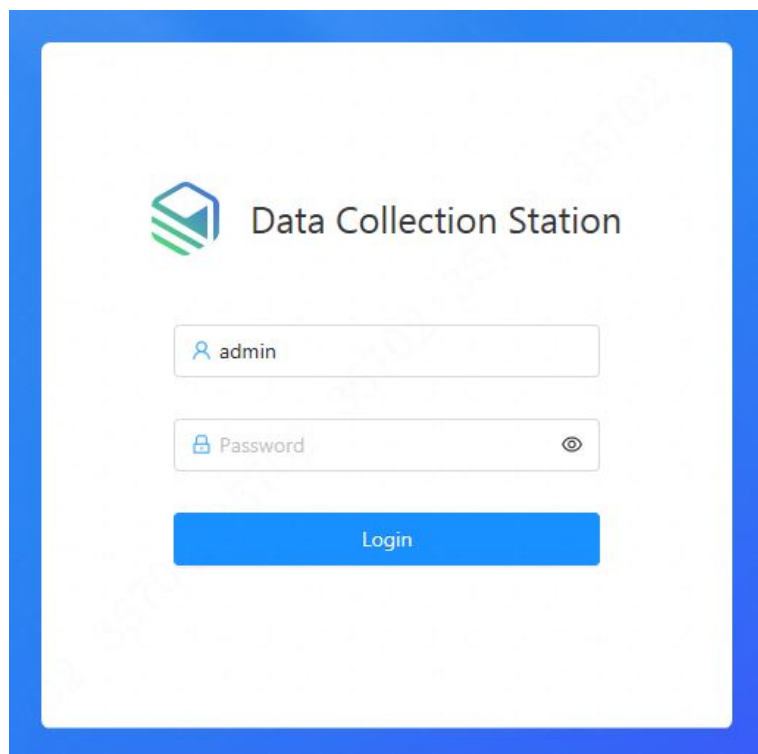
You cannot log in to the Station through browsers without plug-ins.

Log in to the web of the Station as following steps.

Procedure

- Step 1 Enter the IP address (192.168.1.108 for Ethernet 1 and 192.168.2.108 for Ethernet 2 by default) in the address bar of the IE browser, and then press Enter.

Figure 4-67 Login



- Step 2 Enter the username and password.
The administrator account is admin by default.

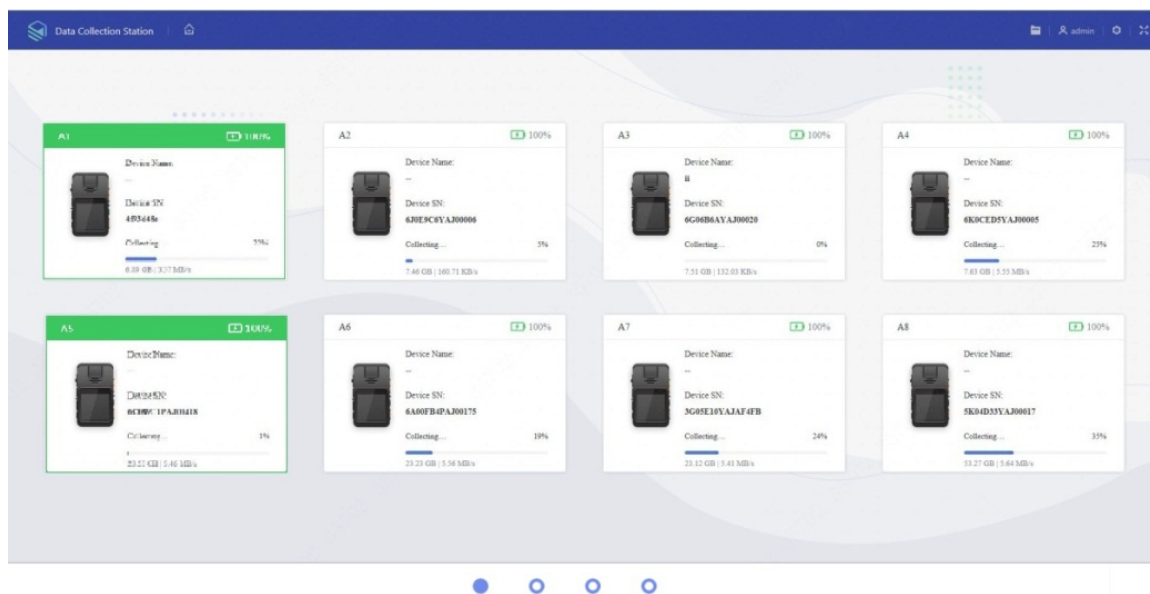
- Step 3 Tap **Login**.

4.2.2 File Management

4.2.2.1 Collecting Files

After collecting data files from body cameras, the Station will upload the files to the platform or FTP according to the configuration in **Storage**.

Figure 4-68 Upload files



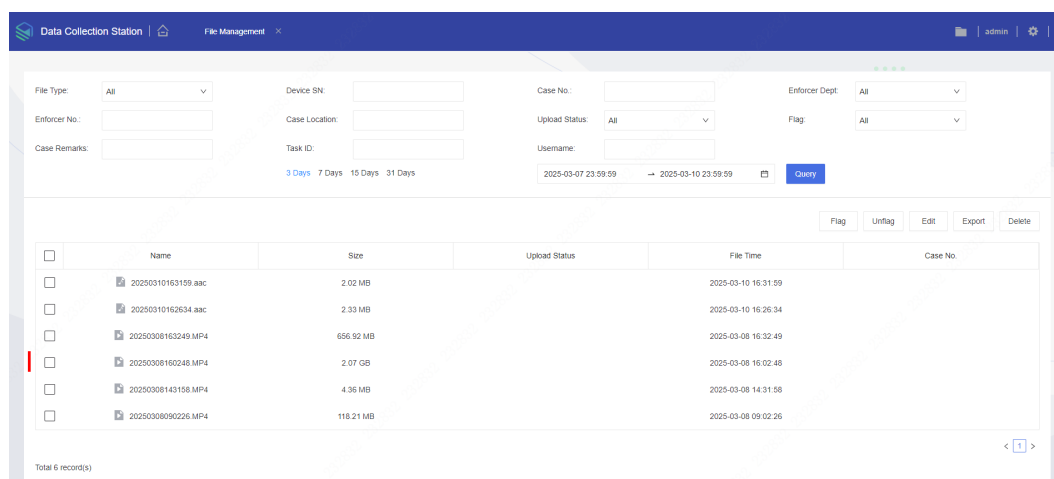
4.2.2.2 Searching for Files

Select **File Management**, and enter file type, enforcer department, upload status, device SN, enforcer No, flag, case No., case location, case remarks task ID and username, and you can search for video files, audio files and snapshots according to the configured conditions.



The maximum time range for file searching is 1 month.

Figure 4-69 Search for files



4.2.2.3 Viewing Files

Double-tap a file to view the details, and you can do the operations of fast play, slow play, zoom in or zoom out.



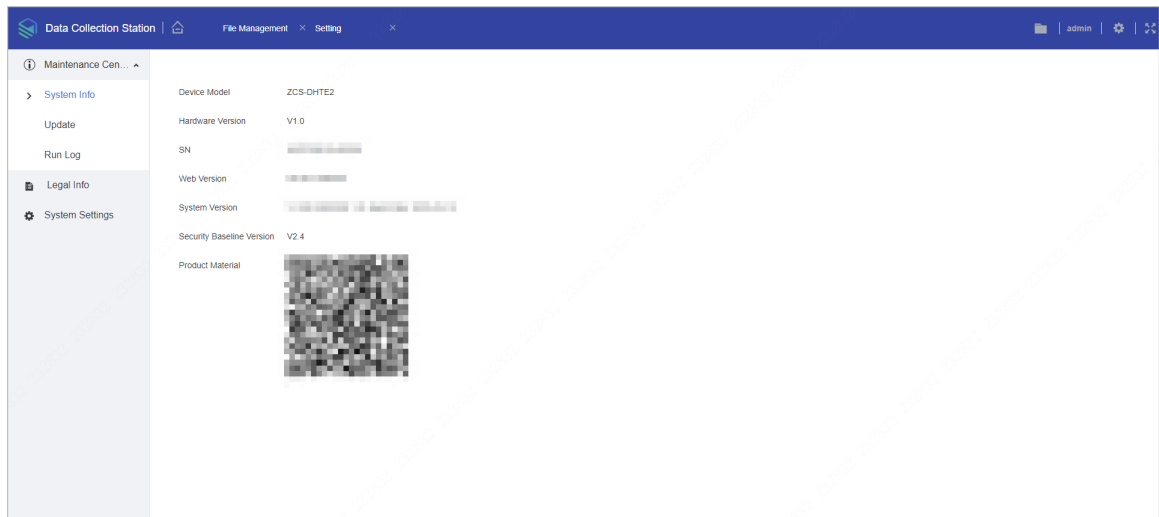
You cannot fast play or slow play an audio file in AMR format.

4.2.3 Configuring Web

4.2.3.1 System Information

Select **Setting** > **Maintenance Center** > **System Info**, and you can view device model, hardware version, SN, web version, system version and security baseline version.

Figure 4-70 System information



4.2.3.2 System Update



- Do not disconnect the power or network, or restart or shutdown the Station during update.
- Make sure that the upgrade file is correct. Improper upgrade file might result in device error.

1. Select **Setting** > **Maintenance Center** > **Update**, select the .bin file, and then tap **Update**.

2. • Auto update

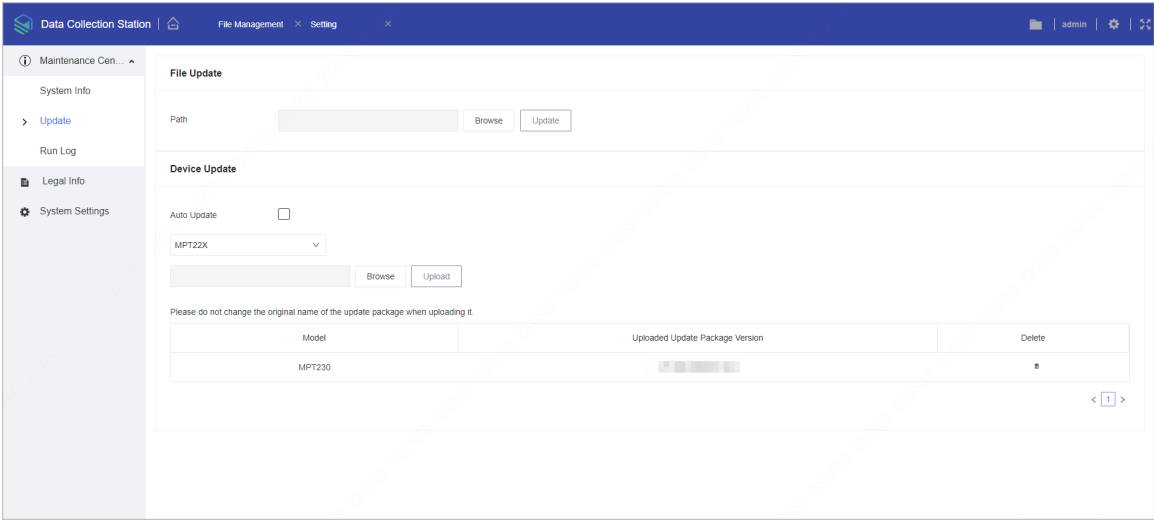
Enable **Auto Update**. When the body camera connects to the collection station, it will automatically detect files and update them.

- 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 4-71 Update



4.2.3.3 Log Running

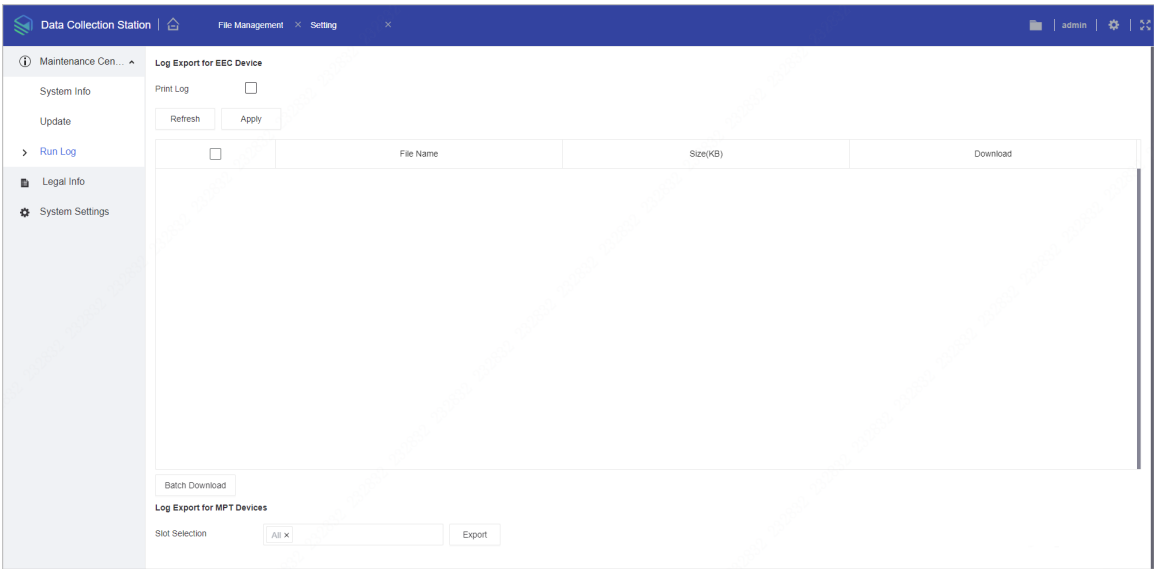
Select **Setting > Maintenance Center > Run Log**.



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 4-72 Run log



4.2.3.4 Legal Information

Select **Setting** > **Maintenance Center** > **Legal Info**. Click **View** to check the open source software notice, software usage license agreement, and privacy policy separately.

Figure 4-73 Legal information



4.2.3.5 System Settings

Select **Setting** > **Maintenance Center** > **System Settings**. Click **View** to check the open source software notice, software usage license agreement, and privacy policy separately.

Appendix 1 RAID

RAID is an abbreviation for Redundant Array of Independent Disks. It is to combine several independent HDDs (physical HDD) to form an HDD group (logic HDD), to provide higher storage performance and data redundancy.

RAID Level

Comparing with one HDD, RAID provides more storage capacity and data redundancy. The different redundant arrays have different RAID level. Each RAID level has its own data protection, data availability and performance degree.

Appendix Table 1-1 RAID level

RAID Level	Description	Min. HDD Needed
RAID 0	RAID 0 is so called striping. RAID 0 is to save the continued data fragmentation on several HDDs. It can process the read and write at the same time, so its read/write speed is N (N refers to the HDD amount of the RAID 0) times as many as one HDD. RAID 0 does not have data redundant, so one HDD damage might result in data loss that cannot be restored.	2
RAID 1	It is also called mirror or mirroring. RAID 1 data is written to two or multiple HDDs equally, which guarantees the system reliability, and the data can be repaired. RAID 1 read speed is almost close to the total volume of all HDDs. The write speed is limited by the slowest HDD. At the same time, the RAID 1 has the lowest HDD usage rate. It is only 50%.	

RAID Level	Description	Min. HDD Needed
RAID 5	RAID 5 is to save the data and the corresponding odd/even verification information to each HDD of the RAID 5 group and save the verification information and corresponding data to different HDDs. When one HDD of the RAID 5 is damaged, system can use the rest data and corresponding verification information to restore the damaged data. It does not affect data integrity.	3
RAID 6	Based on the RAID 5, RAID 6 adds one odd/even verification HDD. The two independent odd/even systems adopt different algorithms, the data reliability is very high. Even two HDDs are broken at the same time, there is no data loss risk. Comparing to RAID 5, the RAID 6 needs to allocate larger HDD space for odd/even verification information, so its read/write is even worse.	4
RAID 10	RAID 10 is a combination of the RAID 1 and RAID 0. It uses the extra high speed efficient of the RAID 0 and high data protection and restores capability of the RAID 1. It has high read/write performance and security. However, the RAID 10 HDD usage efficiency is as low as RAID 1.	

RAID Capacity



CapacityN refers to the mini HDD amount to create the corresponding RAID, which is subject to the value on the web page.

Appendix Table 1-2RAID capacity

Parameter	Total Space of the N HDD
RAID 10	$(N/2) \times \min(\text{capacityN})$

Parameter	Total Space of the N HDD
RAID 6	$(N-2) \times \min(\text{capacity}N)$
RAID 5	$(N-1) \times \min(\text{capacity}N)$
RAID 1	$\min(\text{capacity}N)$
RAID 0	The total amount of current RAID group

Appendix 2 Cybersecurity Recommendations

Mandatory actions to be taken for basic device 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 device (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 device 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 device network security:

1. Physical Protection

We suggest that you perform physical protection to device, especially storage devices. 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, unauthorized connection of removable device (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 device 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 device, 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 device 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 device, 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 device 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 networks.
- Enable IP/MAC address filtering function to limit the range of hosts allowed to access the device.