Data Collection Station

Quick Start Guide

V1.0.1

Foreword

Safety Instructions

The following categorized signal words with defined meaning 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, lower performance, or unpredictable result.
TIPS	Provides methods to help you solve a problem or save you time.
NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.1	Updated "1.1 Introduction."	May 2021
V1.0.0	First release.	March 2021

Important Safeguards and Warnings

This chapter describes the contents covering proper handling of the Data Collection Station (hereafter refer to as "the Station"), hazard prevention, and prevention of property damage. Read these contents carefully before using the Station, comply with them when using, and keep the manual well for future reference.

Operation Requirement

- Do not place or install the Station in a place exposed to sunlight or near the heat source.
- Keep the Station away from dampness, dust or soot.
- Keep the Station installed horizontally on the stable place to prevent it from falling.
- Do not drop or splash liquid onto the Station, and make sure that there is no object filled with liquid on the Station to prevent liquid from flowing into the Station.
- Install the Station in a well-ventilated place, and do not block the ventilation of the Scanner.
- Operate the Station within the rated range of power input and output.
- Do not disassemble the Station.
- Transport, use and store the Station under the allowed humidity and temperature conditions.

Electrical Safety

- Always replace with the same type of batteries.
- Use the recommended power cables in the region and conform to the rated power specification.
- Use the power adapter provided with the Station; otherwise, it might result in people injury and device damage.
- The power source shall conform to the requirement of the Safety Extra Low Voltage (SELV) standard, and supply power with rated voltage which conforms to Limited Power Source requirement according to IEC60950-1. Please note that the power supply requirement is subject to the device label.
- Connect the Station (I-type structure) to the power socket with protective earthing.
- The appliance coupler is a disconnection device. When using the coupler, keep the angle for easy operation.

Table of Contents

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 Portable Mobile Center Platform, the Station can authorize the body camera, 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. It is featured with:

- Recharge and collect data from maximum 32 body cameras at the same time
- Automatically or manually upgrade body cameras.
- Automatically create archive and then save the collected electronic data.
- Automatically upload the evidence to FTP or Portable Mobile Center Platform.
- Automatically synchronize time.
- When there are more than 1 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.

1.2 Product Appearance

1.2.1 Control Module

Figure 1-1 Front panel and rear panel

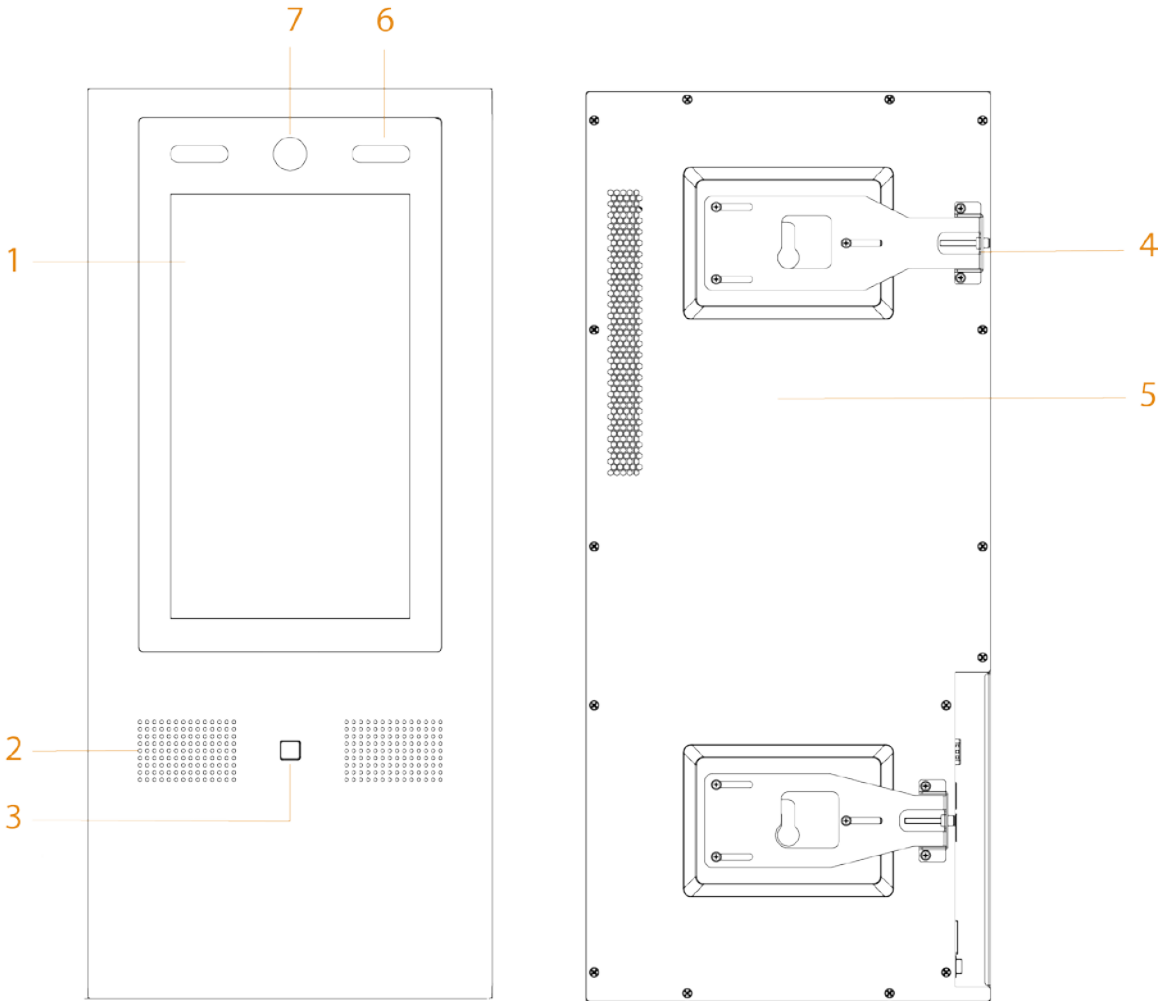


Figure 1-2 Side panel

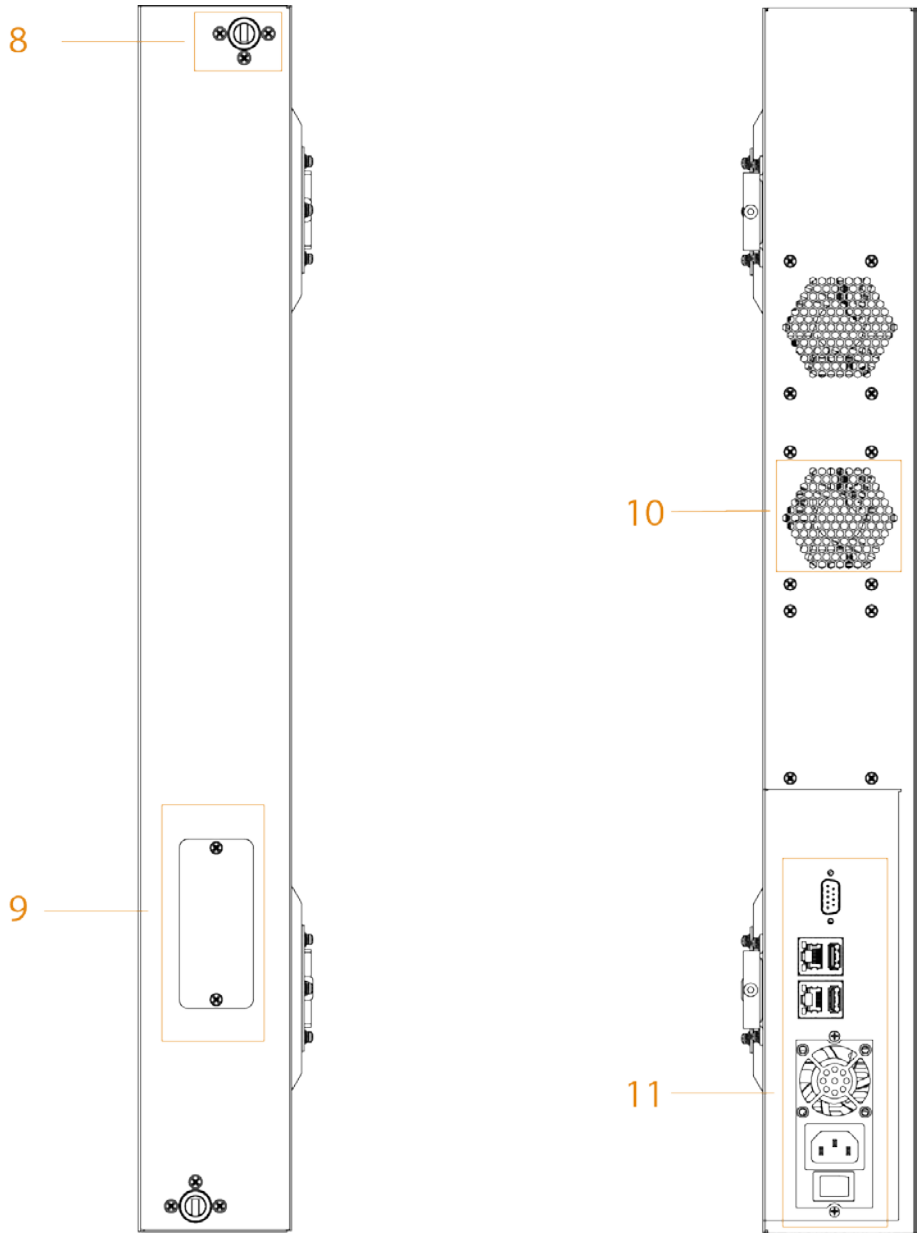


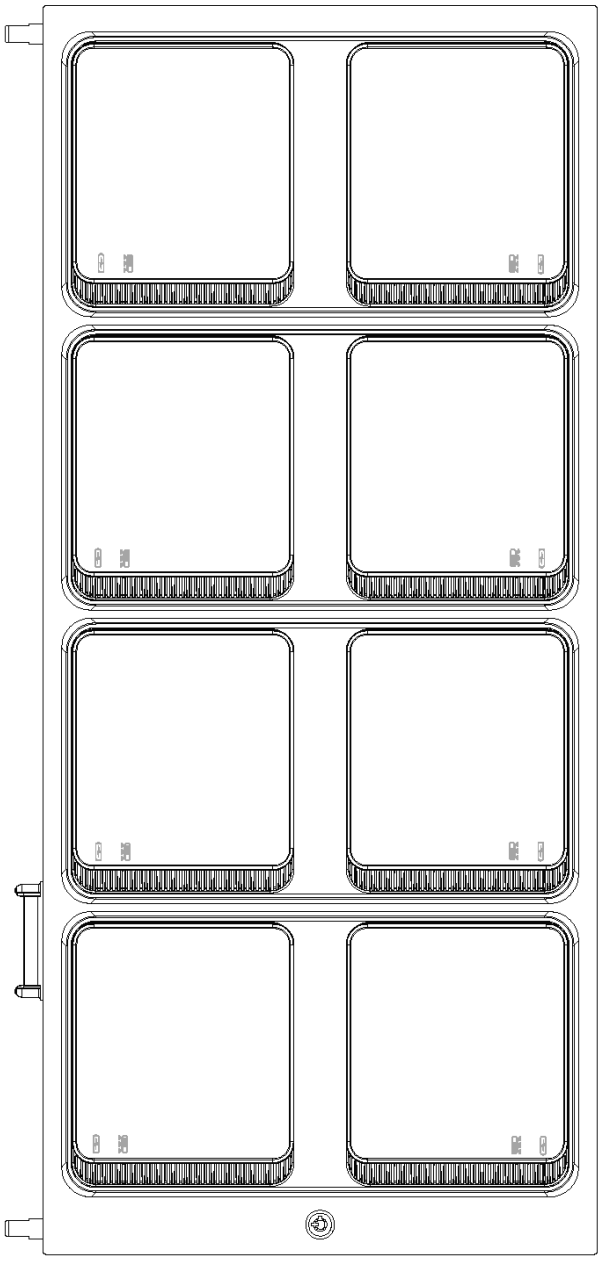
Table 1-1 Appearance description

No.	Name	Description
1	Touch screen	13.3-inch touch screen.
2	Speaker	Audio output.
3	Fingerprint sensor	Adds fingerprint data or unlock by fingerprint. At most 3 fingerprints can be added for each user.
4	Adjusting board	Remove the control module when connecting control module and data collection modules.
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 on the top, and the other is at the bottom.

No.	Name	Description
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 Table 1-2.

1.2.2 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 1 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 the dock:  indicates recharging;  indicates collecting data.
- When a dock cannot be opened, you can open it with the key.

1.3 Description of Buttons

Figure 1-4 Ports

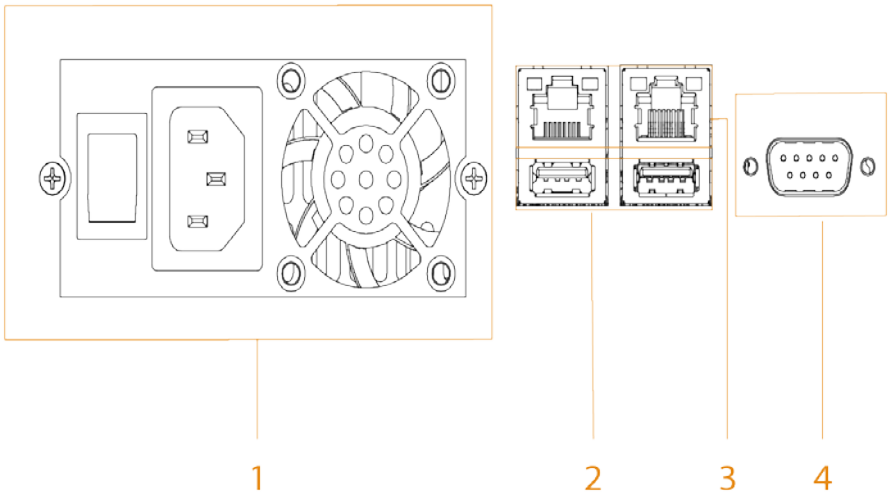


Table 1-2 Port description

No.	Name	Description
1	Power input	Inputs 100 V–240 V AC 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 (USB2.0 and USB3.0), 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.

1.4 Power on

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

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.

1.5 Device Connection

1.5.1 Connecting Control Module and Data Collection Module

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

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.

1.5.2 Connecting Body Camera and Data Collection Module

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 special for MPT220 body camera by default. If you want to use for MPT210 body camera, use the separate slot in the accessories package.

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

Do not drag the data cable too harsh. Otherwise, it might result in invalid spring or loosening port connection!

Figure 1-5 Take out data cable (MPT220 slot)

Figure 1-6 Take out data cable (MPT210 slot)

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

Figure 1-7 Connect device (MPT220 slot)

Figure 1-8 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 MPT220 body camera, insert the device into the slot.
- For MPT210 body camera, insert the clip into the slot. Only MPT210 body camera with the latest clip can be inserted into the slot. See Figure 1-8.

Figure 1-9 Data collection (MPT220 slot)

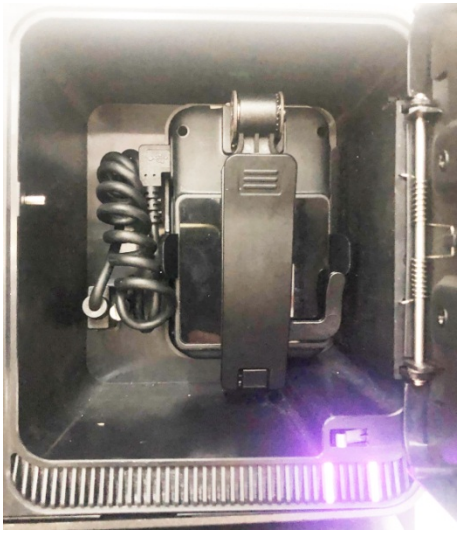


Figure 1-10 Data collection (MPT210 slot)

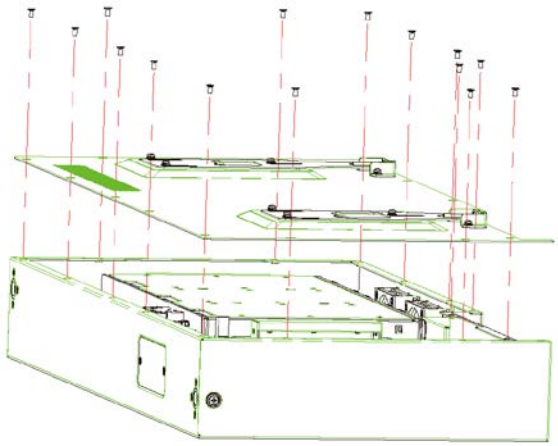
2 HDD Installation

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.

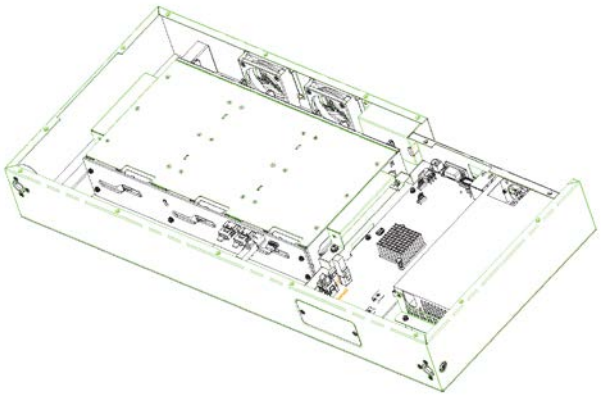
Step 1 Loosen the screws on the rear cover, and then remove the rear cover.

Figure 2-1 Remove rear cover



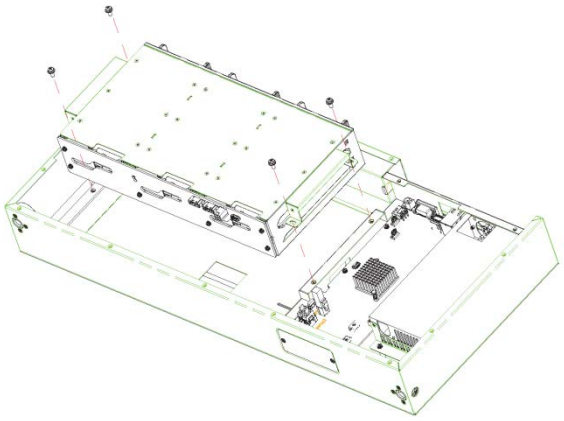
Step 2 Disconnect the cables between main board and HDD plate.

Figure 2-2 Loosen cable



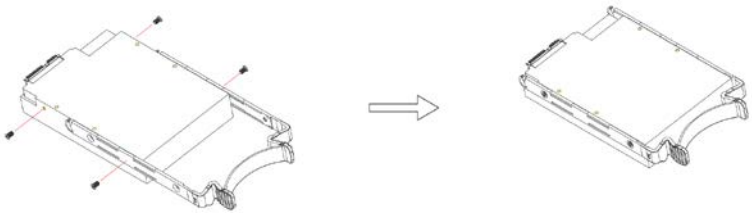
Step 3 Loosen the four fixed screws on the HDD box, and then take out the box.

Figure 2-3 Take out HDD box



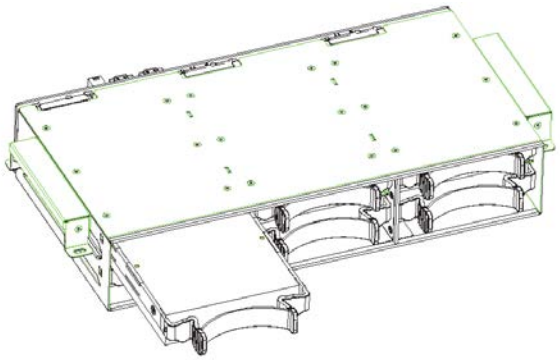
Step 4 Fix HDDs

Figure 2-4 Fix HDD



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

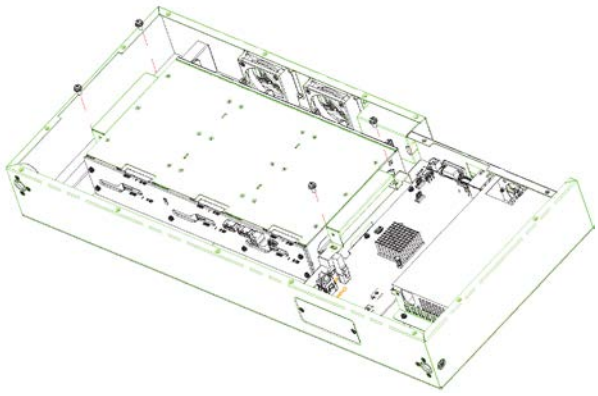
Figure 2-5 Install HDD



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

Step 6 Fix the HDD box in the chassis.

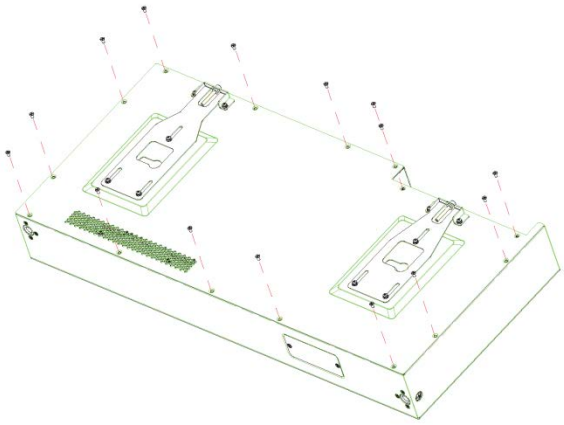
Figure 2-6 Install HDD box



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

Step 8 Fix the cover.

Figure 2-7 Fix the cover



3 Configuration and Operation

Figure 3-1 Main interface

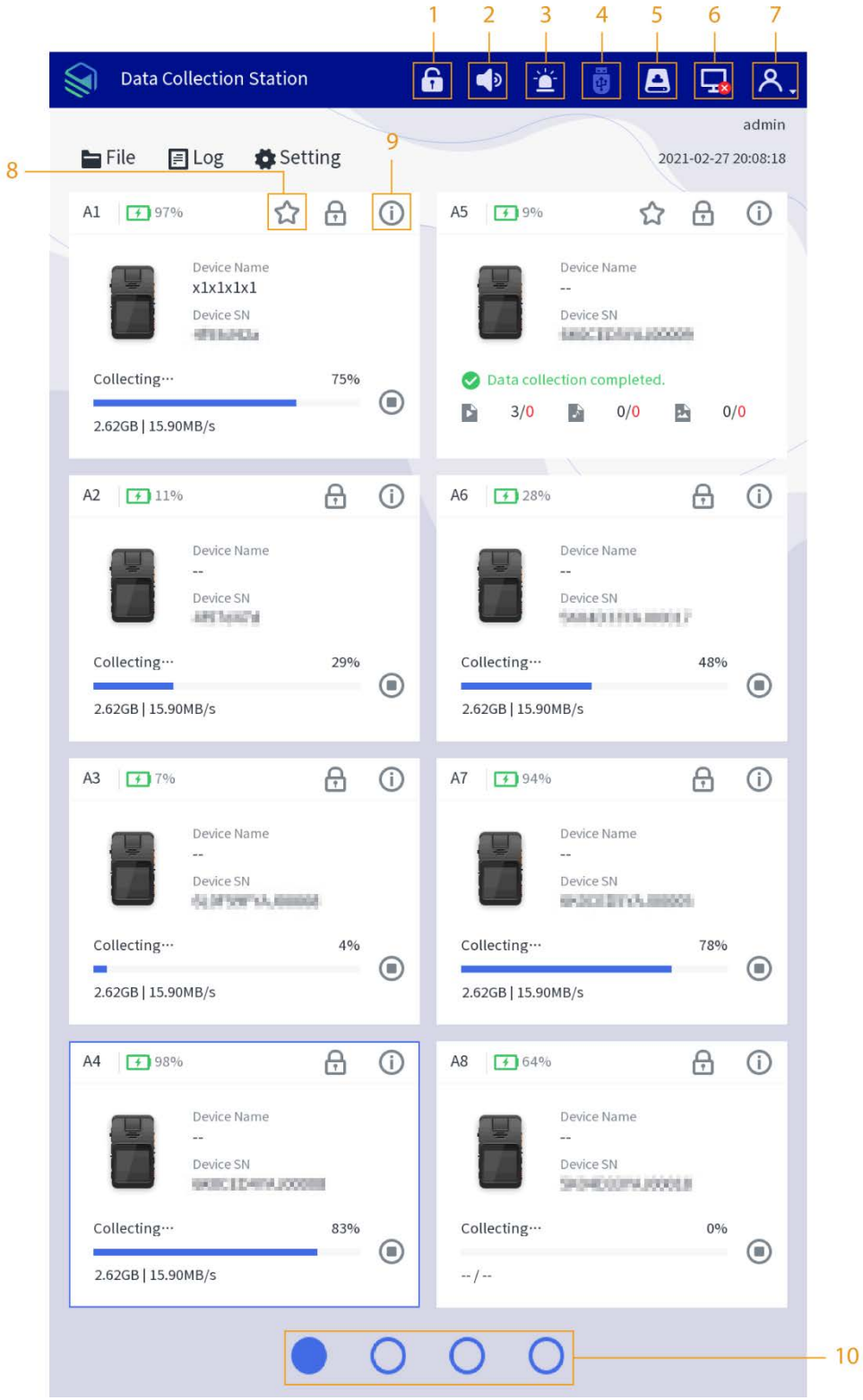


Table 3-1 Main interface description

No.	Description
1	Unlock the dock by one tap.
2	Alarm. Tap it, and the alarm tune is disabled.

No.	Description
3	Alarm information display. The red light flashes when there is alarm.
4	External USB storage device. Grey means no USB storage device is connected.
5	View HDD capacity.
6	: Indicates a file is being uploaded; : Indicates no file is being uploaded.
7	Login, logout, restart, shutdown, and editing the user information.
8	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.
9	View update methods of the Station and body cameras. Click **Bind Enforce** on the **Device Info** interface, enter the enforcer name and enforcer No., click **Search**, and then select the enforcer that you want to bind.
10	Switch interfaces of data collection modules. It supports 4 interfaces at most.

3.1 File Management

3.1.1 File Collection

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

3.1.2 Viewing Files

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

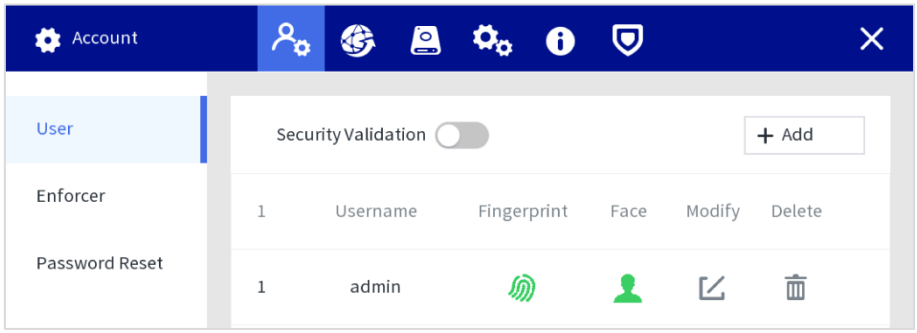
3.2 User

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

3.2.1 User Management

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

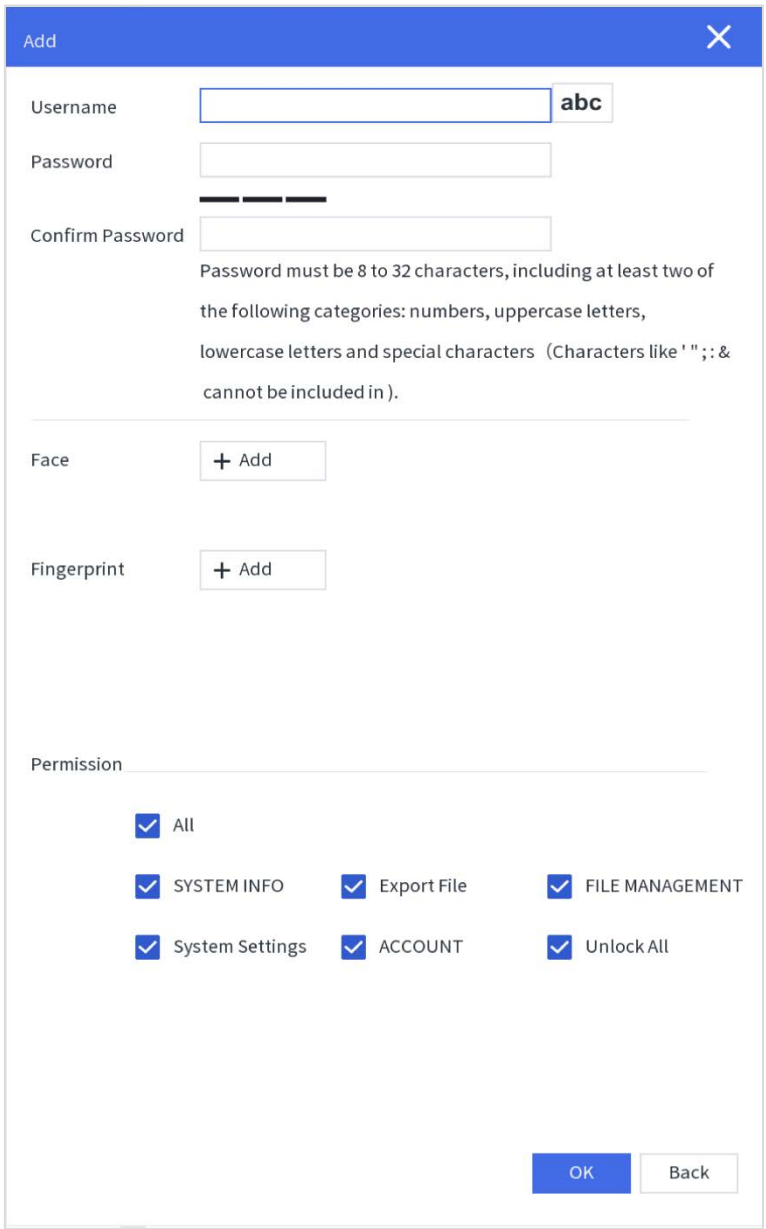
Figure 3-2 User management



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

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

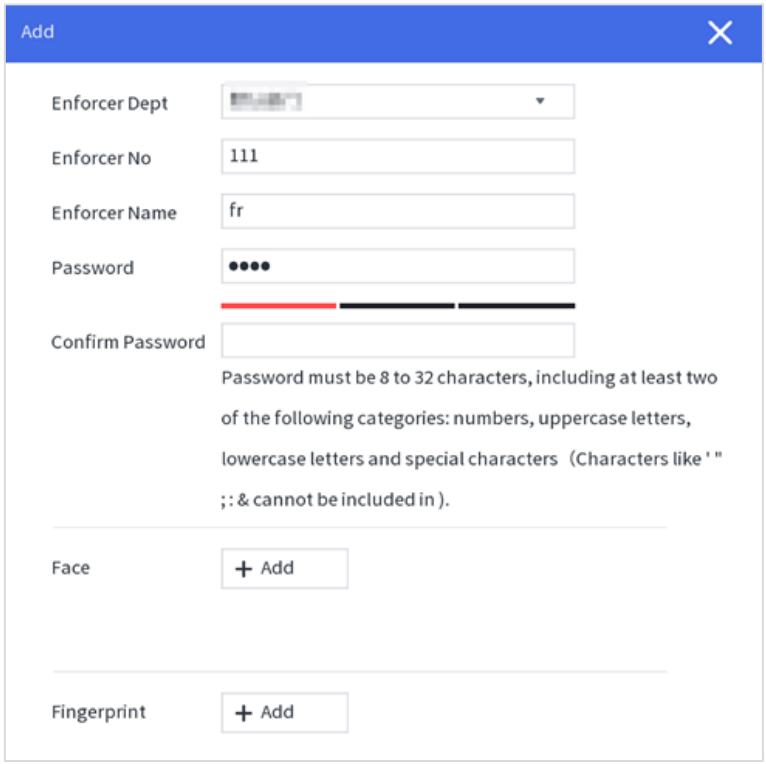
Figure 3-3 Add users



3.2.2 Adding Enforcer

Select **Setting** > **Account** > **Enforcer**, and then click **Add** to add users. Enter enforcer department, enforcer No., enforcer name, password, and confirm password, and add face and fingerprint as needed.

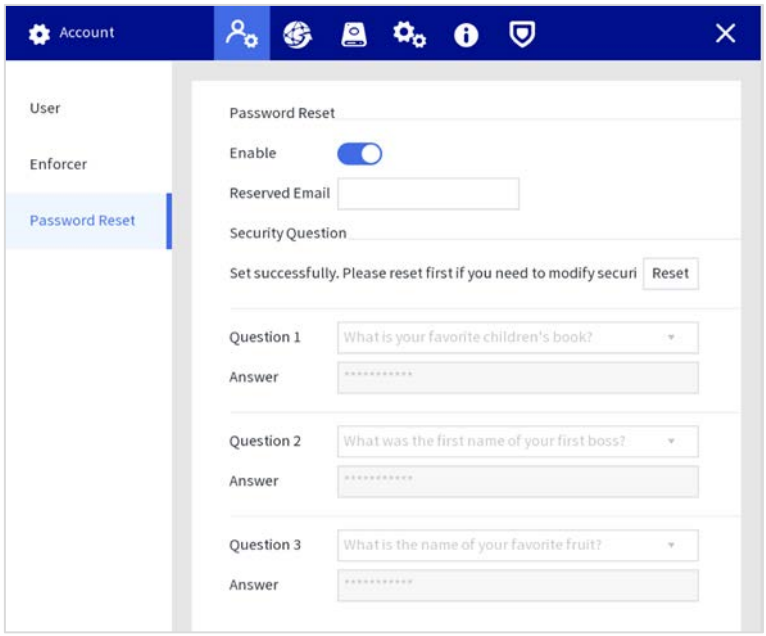
Figure 3-4 Adding enforcer



3.2.3 Resetting Password

Select **Setting** > **Account** > **Password Reset**, and enter the recovery email address and the security questions.

Figure 3-5 Resetting password



Appendix 1 Cybersecurity Recommendations

Cybersecurity is more than just a buzzword: it's something that pertains to every device that is connected to the internet. IP video surveillance is not immune to cyber risks, but taking basic steps toward protecting and strengthening networks and networked appliances will make them less susceptible to attacks. Below are some tips and recommendations on how to create a more secured security system.

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.