

Data Collection Station

Quick Start Guide



V1.0.0

Foreword

General

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

Safety Instructions

The following signal words might appear in the manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, reductions in performance, or unpredictable results.
 TIPS	Provides methods to help you solve a problem or save time.
 NOTE	Provides additional information as a supplement to the text.

Revision History

Version	Revision Content	Release Time
V1.0.0	First release.	May 2023

Privacy Protection Notice

As the device user or data controller, you might collect the personal data of others such as their face, 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 whiteboard, hazard prevention, and prevention of property damage. Read carefully before using the whiteboard, and comply with the guidelines when using it.

Transportation Requirements



Transport the device under allowed humidity and temperature conditions.

Storage Requirements



Store the device under allowed humidity and temperature conditions.

Installation Requirements



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

Operation Requirements



WARNING

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



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

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

Maintenance Requirements



Do not disassemble the device without professional instruction.

Contents

Foreword.....	I
Important Safeguards and Warnings.....	III
1 Introduction.....	1
1.1 Dimensions.....	1
1.2 Ports.....	2
1.3 Power on.....	3
2 HDD Installation.....	4
3 Configuration and Operation.....	7
3.1 Device Initialization.....	8
3.2 Login.....	9
3.3 File Management.....	9
3.3.1 File Collection.....	9
3.3.2 Viewing Files.....	10
3.4 Account Management.....	11
3.4.1 Adding the User.....	11
3.4.2 Adding the Enforcer.....	12
3.4.3 Resetting Password.....	13
Appendix 1 Cybersecurity Recommendations.....	15

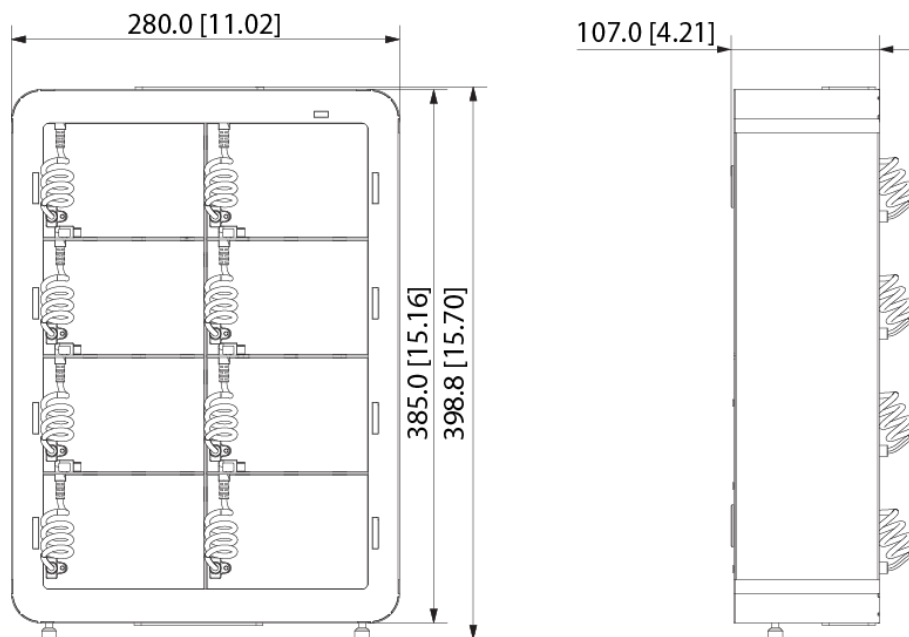
1 Introduction

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

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

1.1 Dimensions

Figure 1-1 Dimensions (mm [inch])



1.2 Ports

Figure 1-2 Ports (1)

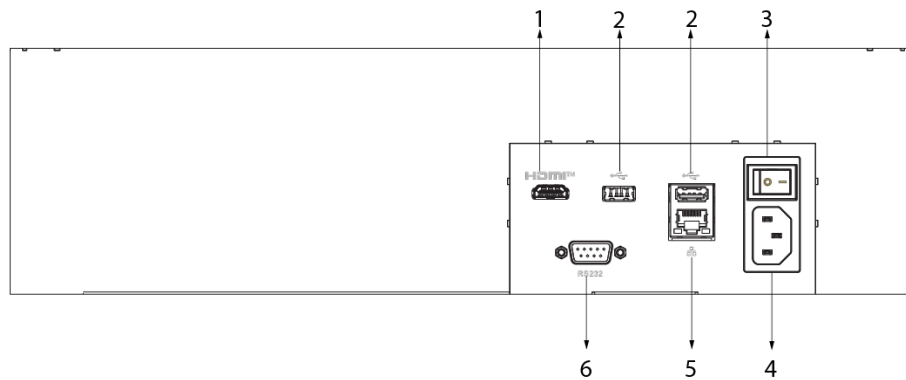


Figure 1-3 Port 2

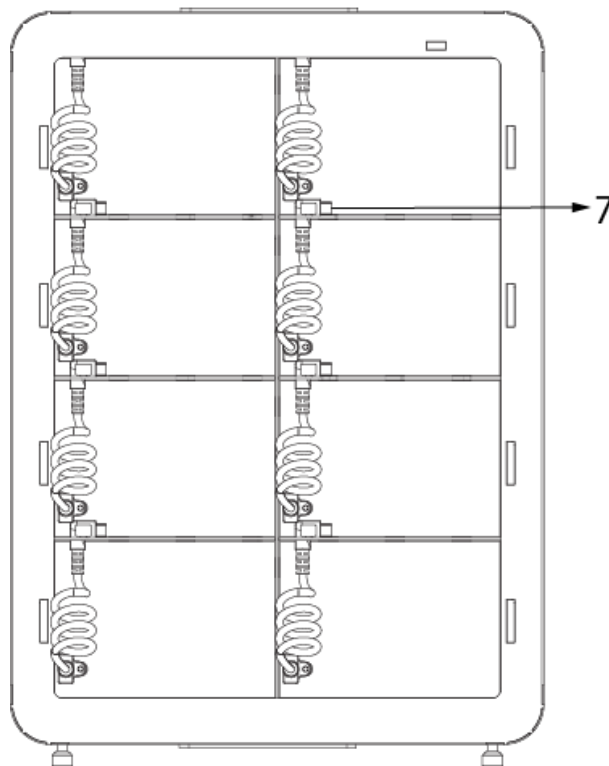


Table 1-1 Ports description

No.	Name	Description
1	HDMI	Inputs uncompressed high definition (HD) video signals and multichannel audio signals from the external HDMI sources. Supports 1080p@60 Hz.
2	USB ports	Connect to USB storage devices (USB 2.0 and USB 3.0) and mouse.
3	Power switch	Turn on or turn off the Station.
4	Power input	Inputs 100 –240 VAC power for the Station.

No.	Name	Description
5	Ethernet	Gigabit network.
6	RS-232	Used for common serial debugging, IP address configuration and data transmission of transparent serial.
7	USB ports	Connects 8 body cameras.

1.3 Power on

Procedure

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

Step 2 Press the power button.

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

2 HDD Installation

You can install 4 HDDs (hard disk drives).



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

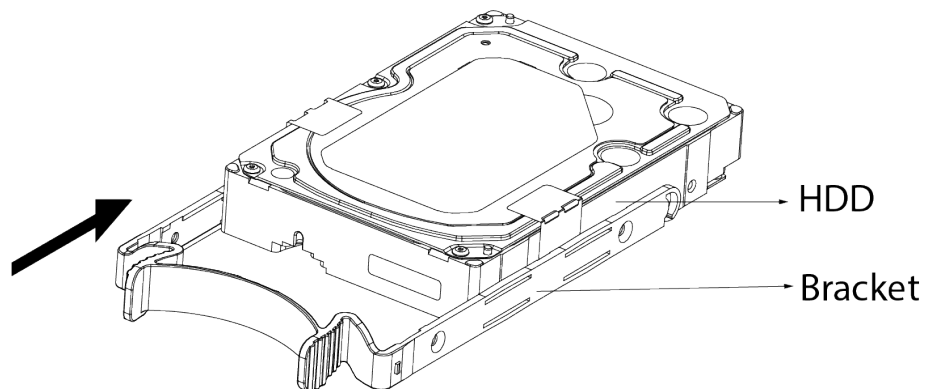


- To avoid insufficient storage space, HDDs larger than 2 TB are recommended.
- To reduce the writing pressure of each HDD, we recommend you to install at least 2 HDDs with the same capacity for data collection and recharging.

Procedure

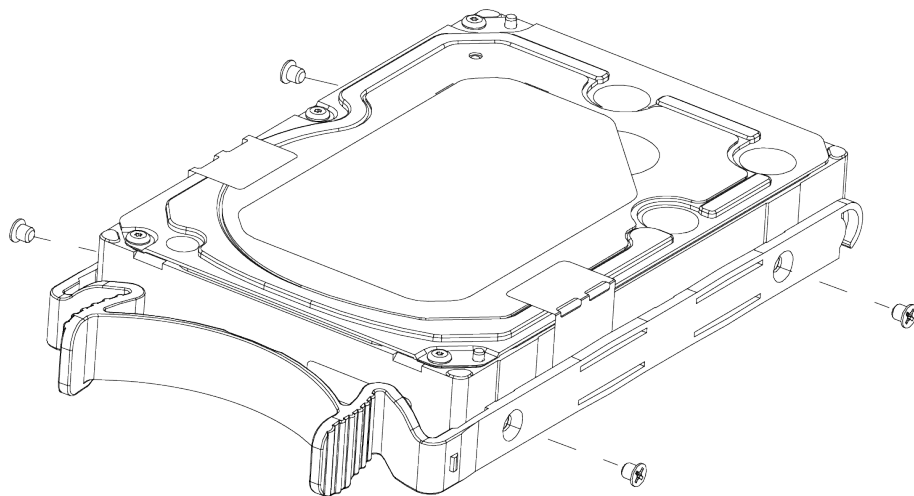
Step 1 Put the bracket flat on the desktop, and then install the HDD horizontally into the bracket.

Figure 2-1 Install the HDD



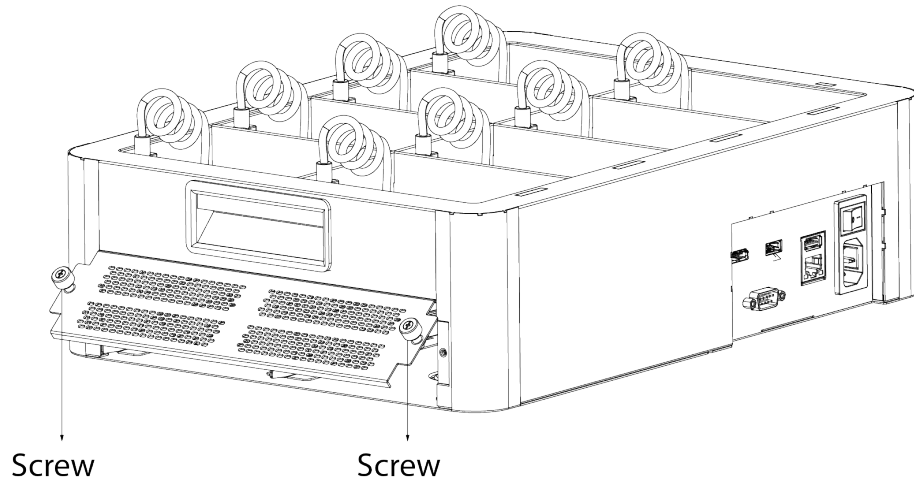
Step 2 Tighten the 4 screws on the bracket.

Figure 2-2 Tighten the screws



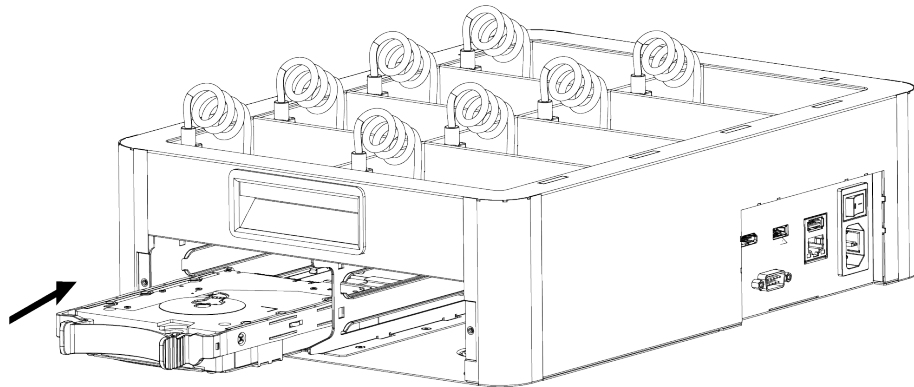
Step 3 Loosen the following screws to the leftward, and then hold the screws and rotate them outward to detach the cover.

Figure 2-3 Detach the cover



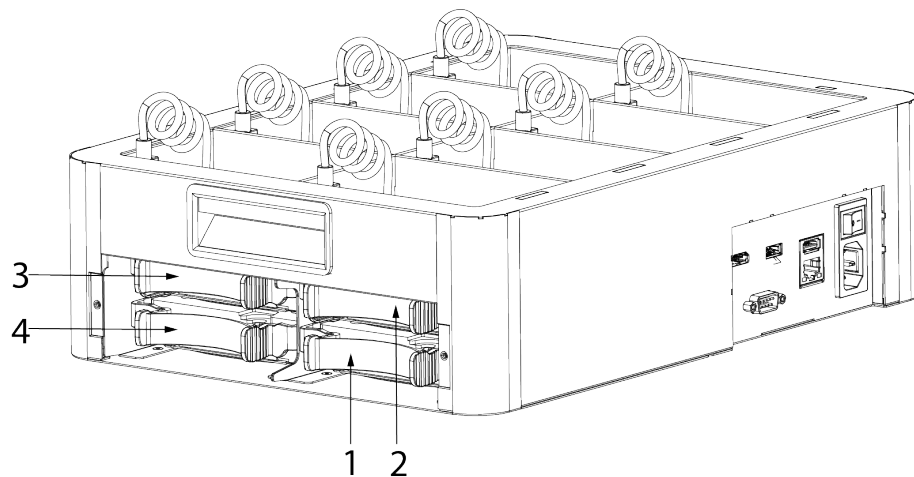
Step 4 Push the HDD with bracket installed into the chassis guide rails.

Figure 2-4 Install the bracket to the chassis



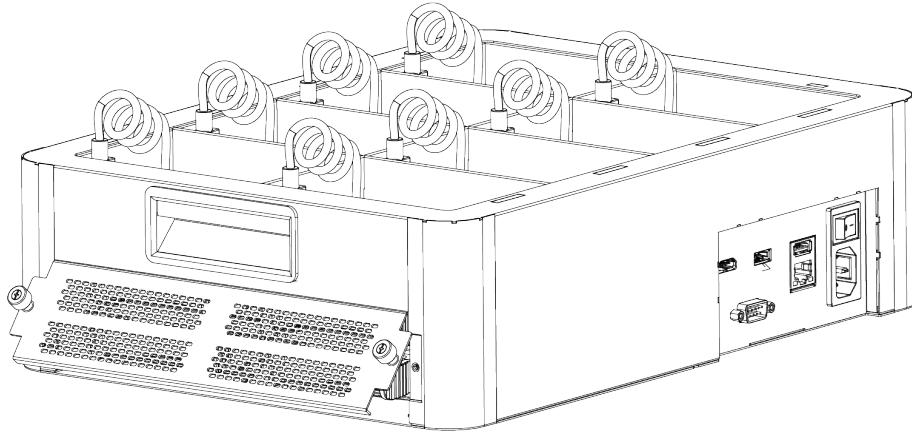
Step 5 (Optional) Repeat step 1, step 2 and step 4 to add more HDDs.

Figure 2-5 4 HDDs installation



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

Figure 2-6 Install the cover



3 Configuration and Operation

Figure 3-1 Home screen

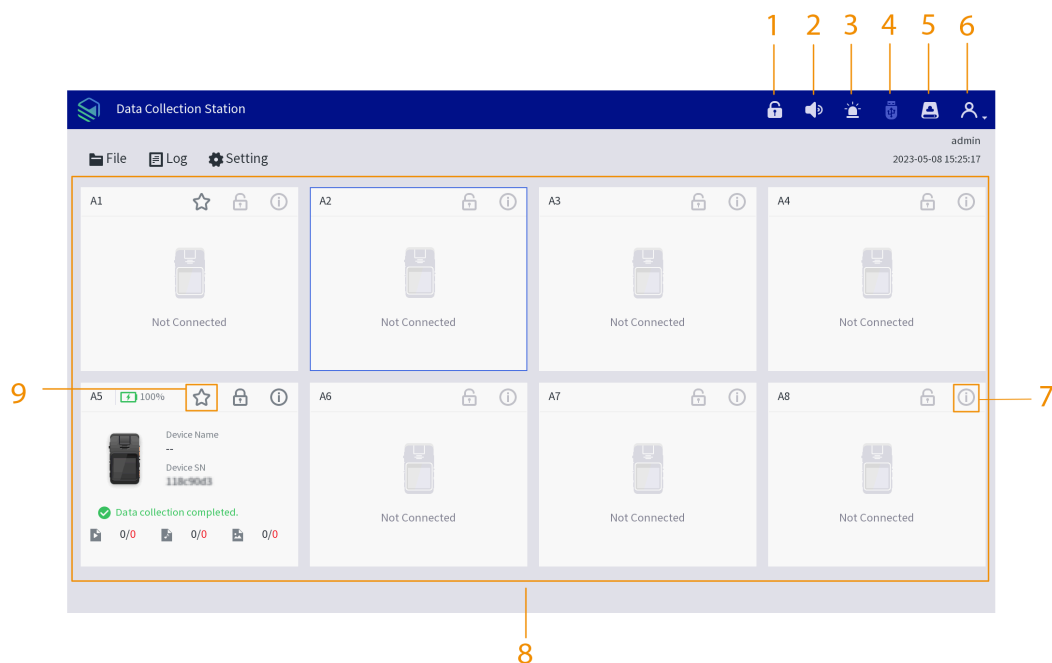
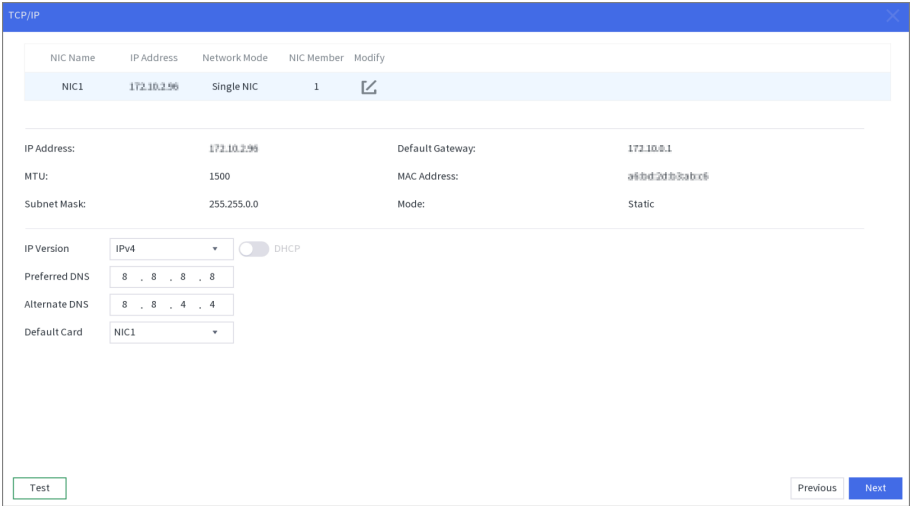


Table 3-1 Home screen description

No.	Description
1	Unlock the Station with one tap.  Click  on a different body camera's page to unlock the specific body camera.
2	Alarm. Tap it, and the alarm tune is turned off.
3	Alarm information display. The red light flashes when there is alarm.
4	External USB storage device. ● Grey means no data is being exported. ● Green means data of selected body camera is exporting.
5	View HDD capacity.
6	Login, logout, restart, shutdown, and editing the user information.
7	View update methods of the Station and body cameras.  ● Click Bind Enforce on the Device Info page, enter the enforcer name and enforcer No, click Search, and then select the enforcer that you want to bind.

Step 7 Click  to modify the IP address, and then click **Next**.
The initialization is finished.

Figure 3-3 TCP/IP



NIC Name	IP Address	Network Mode	NIC Member	Modify
NIC1	172.10.2.96	Single NIC	1	

IP Address: 172.10.2.96 Default Gateway: 172.10.2.1
MTU: 1500 MAC Address: 98bd2db3ab36
Subnet Mask: 255.255.0.0 Mode: Static

IP Version: IPv4 ☐ DHCP
Preferred DNS: 8 . 8 . 8 . 8
Alternate DNS: 8 . 8 . 4 . 4
Default Card: NIC1

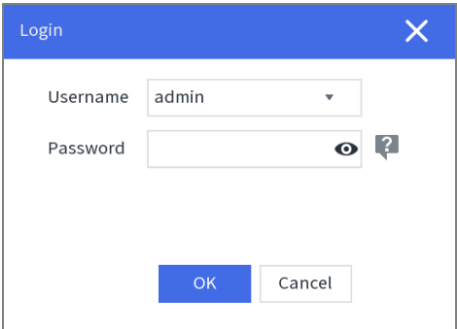
Test Previous Next

3.2 Login

Procedure

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

Figure 3-4 Login



Login

Username admin

Password  

OK Cancel

3.3 File Management

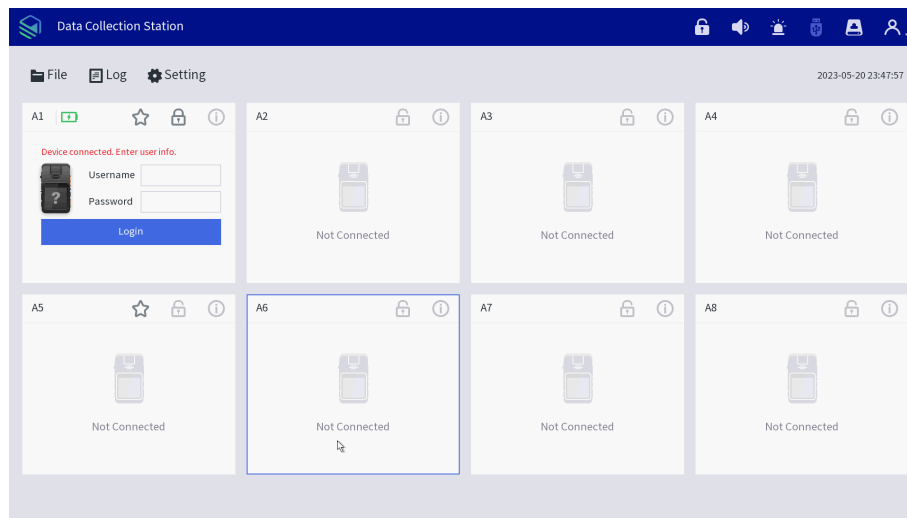
3.3.1 File Collection

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

1. Connect the Station with the body camera.

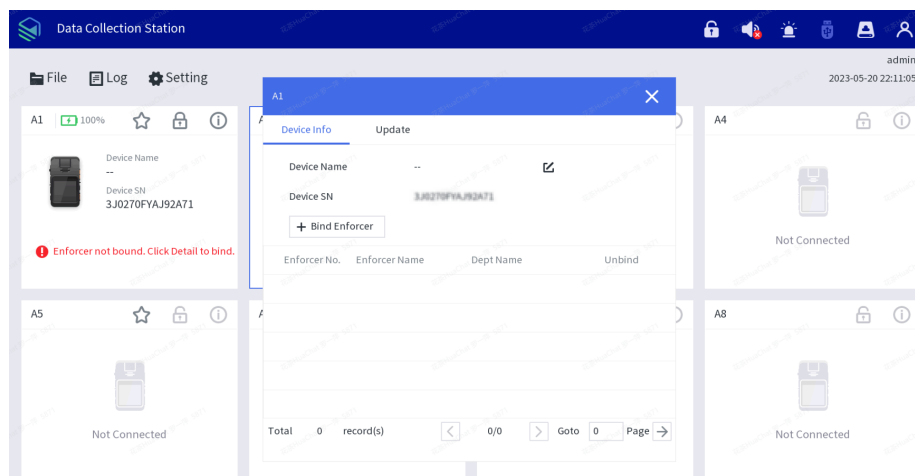
2. Login the Station.
3. Enter the username and password, and then click **Login**.

Figure 3-5 Login the body camera



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

Figure 3-6 Bind enforcer



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

3.3.2 Viewing Files

Procedure

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

Figure 3-7 View files

File

File Type

All

Device SN

Case No.

Enforcer Dept

All

Enforcer No.

Case Location

Upload Status

All

Flag

All

Case Remarks

3 Days

1 Week

15 Days

1 Month

2023-05-05

23:59:59

-

2023-05-08

23:59:59

Query

★ Flag

☆ Unflag

Edit

Export

Delete

☐	Name	Size	Upload	Time	Case No.
☐	20230508103629.mp4	7.24 MB		2023-05-08 10:36:29	
☐	20230426190000.mp4	48.88 MB		2023-04-26 19:00:00	
☐	20230426183000.mp4	109.67 MB		2023-04-26 18:30:00	
☐	20230426180000.mp4	116.53 MB		2023-04-26 18:00:00	
☐	20230426173000.mp4	116.40 MB		2023-04-26 17:30:00	
☐	20230426170000.mp4	80.09 MB		2023-04-26 17:00:00	
☐	20230426163000.mp4	90.73 MB		2023-04-26 16:30:00	

3.4 Account Management

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

3.4.1 Adding the User

Procedure

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

Figure 3-8 User Management

Account

User

Enforcer

Password Reset

+ Add

1	Username	Modify	Delete
1	admin		

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

Set the username and password, and then configure user permissions. All permissions are enabled by default.

Figure 3-9 Add users

Add [X]

Username

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).

Password Expires in Never ▾

Permission

☒ All

☒ SYSTEM INFO ☒ Export File ☒ FILE MANAGEMEN

☒ System Settings ☒ ACCOUNT

OK Back

Step 3 Click **OK**.

Related Operations

- Click  to modify the user information.
- Click  to delete the user.

3.4.2 Adding the Enforcer

Procedure

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

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

Figure 3-10 Add the enforcer

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains the following fields and elements:

- Enforcer Dept:** A dropdown menu currently showing "Reserved Dept".
- Enforcer No.:** A text input field.
- Enforcer Name:** A text input field.
- Password:** A text input field.
- Confirm Password:** A text input field.
- Password Requirement Note:** 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)."
- Buttons:** "OK" and "Back" buttons located at the bottom right.

Step 3 Click **OK**.

3.4.3 Resetting Password

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

Figure 3-11 Reset password

Password Reset

Enable ☒

Reserved Email

Security Question

Admin password can be found after setting security questions.

Question 1

What is your favorite children's book?

▼

Answer

Question 2

What was the first name of your first boss?

▼

Answer

Question 3

What is the name of your favorite fruit?

▼

Answer

Apply

Back

Appendix 1 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.