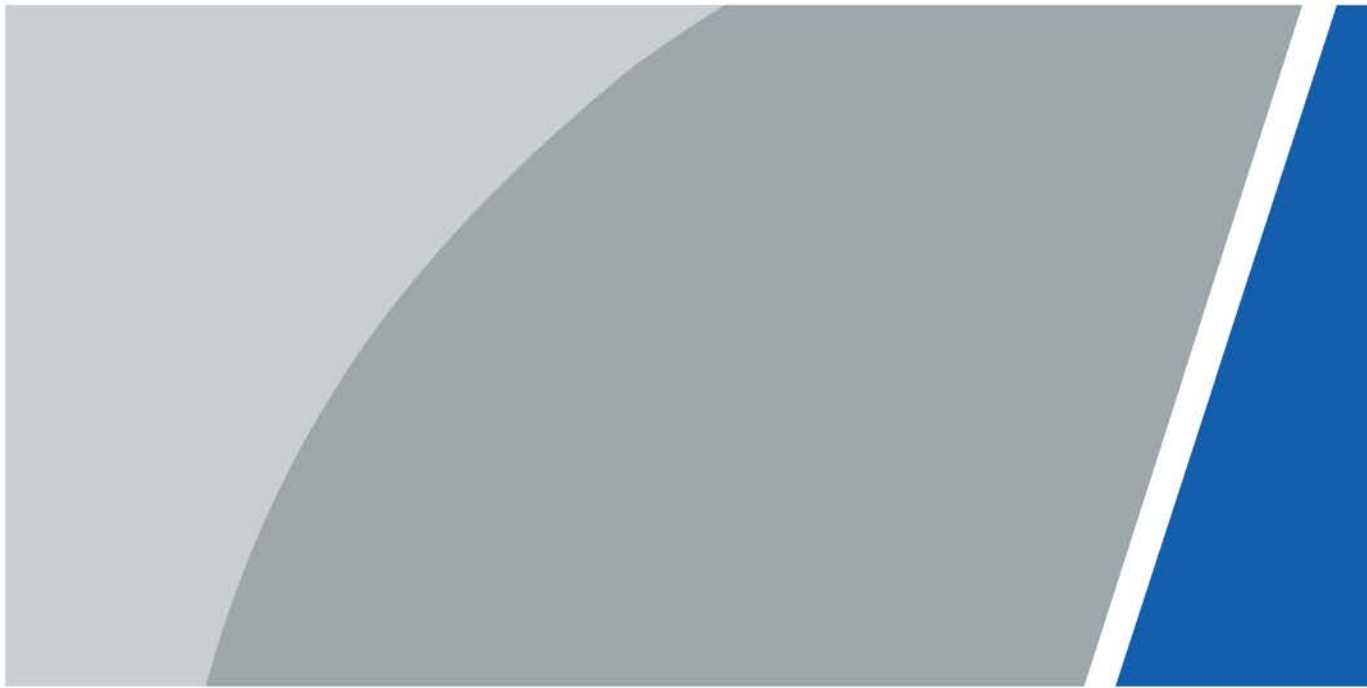


Data Collection Station






User's Manual



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

Foreword	I
Important Safeguards and Warnings	I
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	4
1.4 Description of Buttons	5
1.5 Power on	6
2 Device Connection	1
2.1 Connecting Control Module and Data Collection Module	1
2.2 Connecting Body Camera and Data Collection Module	1
3 HDD Installation	5
4 Configuration and Operation	8
4.1 General	8
4.1.1 File Management	9
4.1.2 Searching for Log	10
4.1.3 Local Settings	12
4.2 Web Configuration	64
4.2.1 Login	64
4.2.2 File Management	64
4.2.3 Configuring Web	66
Appendix 1 RAID	67
Appendix 2 Cybersecurity Recommendations	69

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, 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 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.

1.3 Product Appearance

1.3.1 Control Module

Figure 1-1 Front panel and rear panel

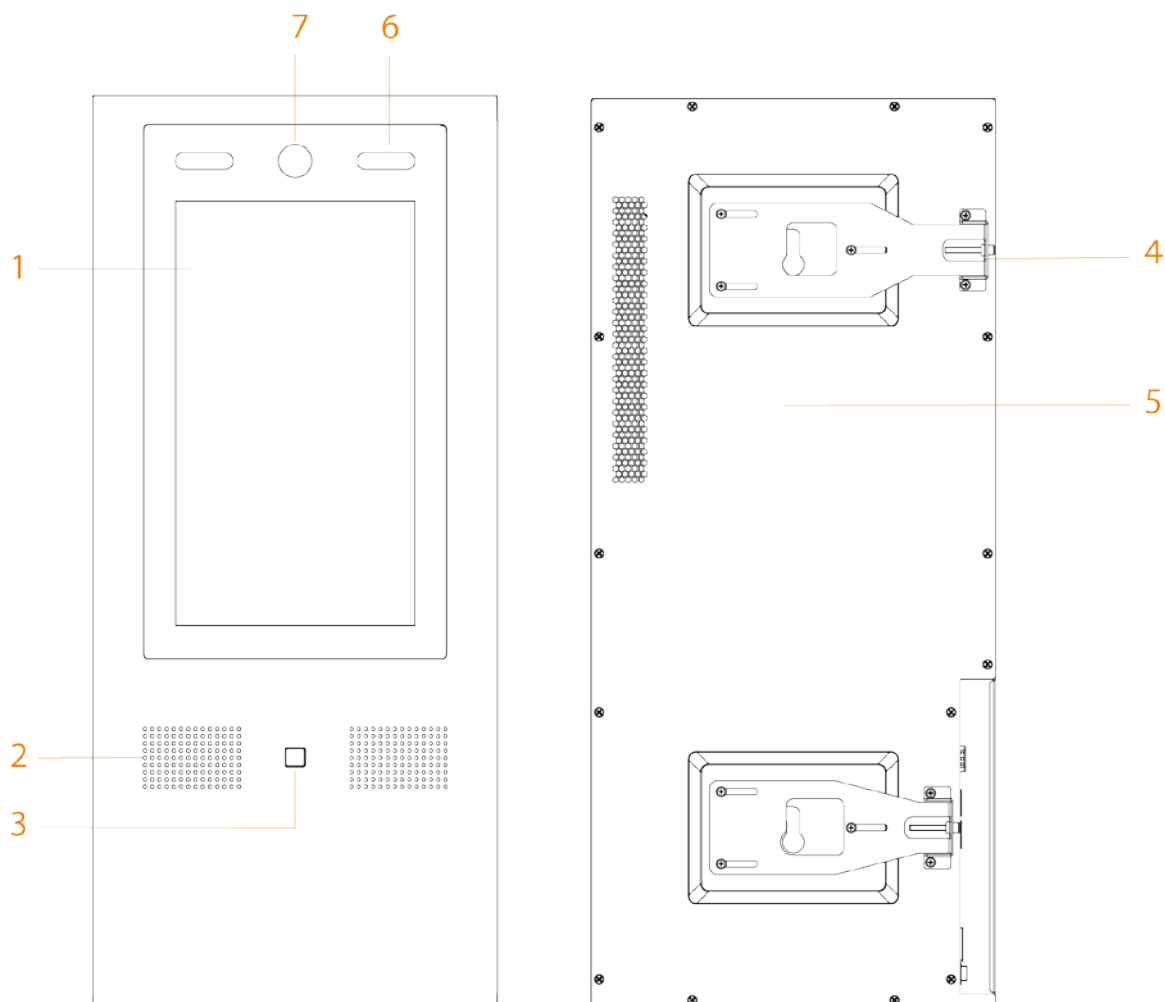


Figure 1-2 Side panel

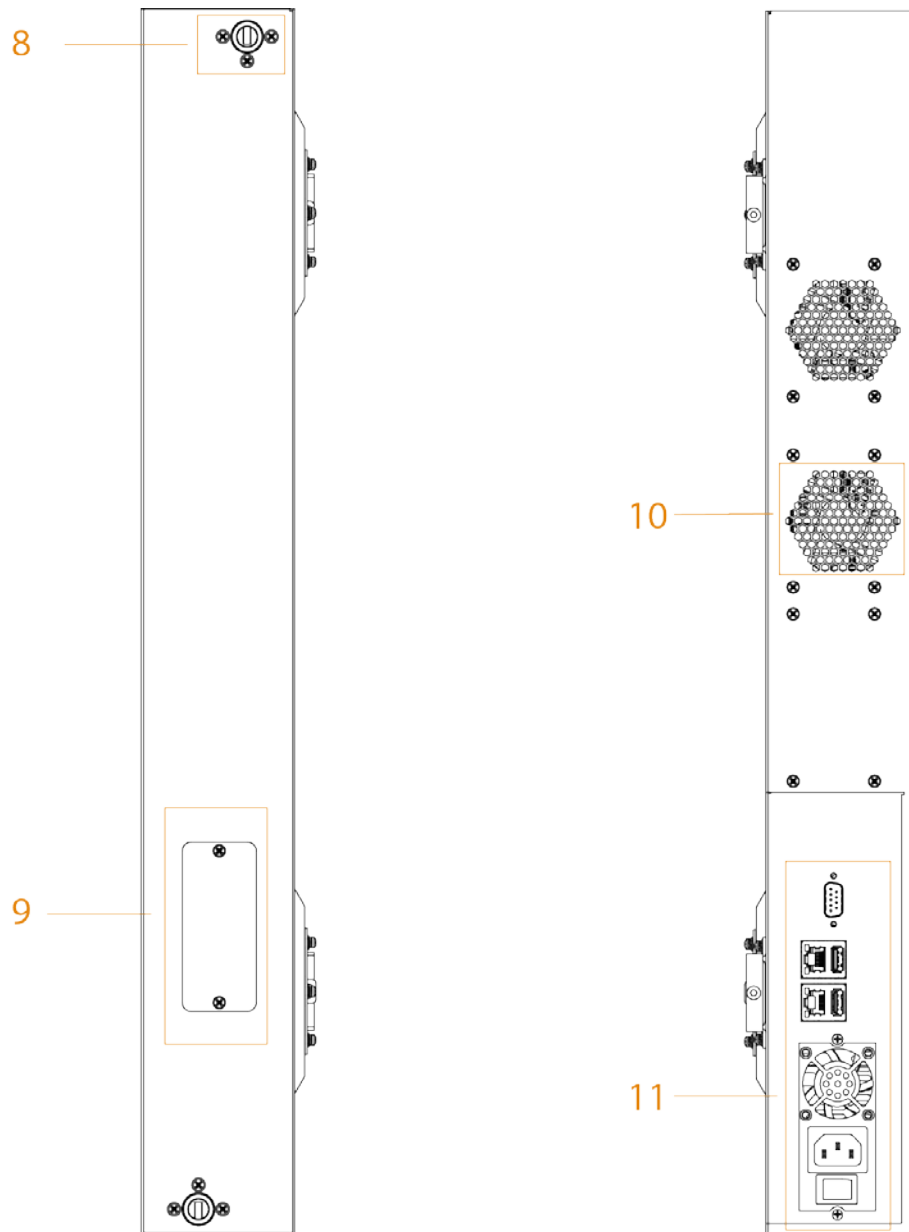


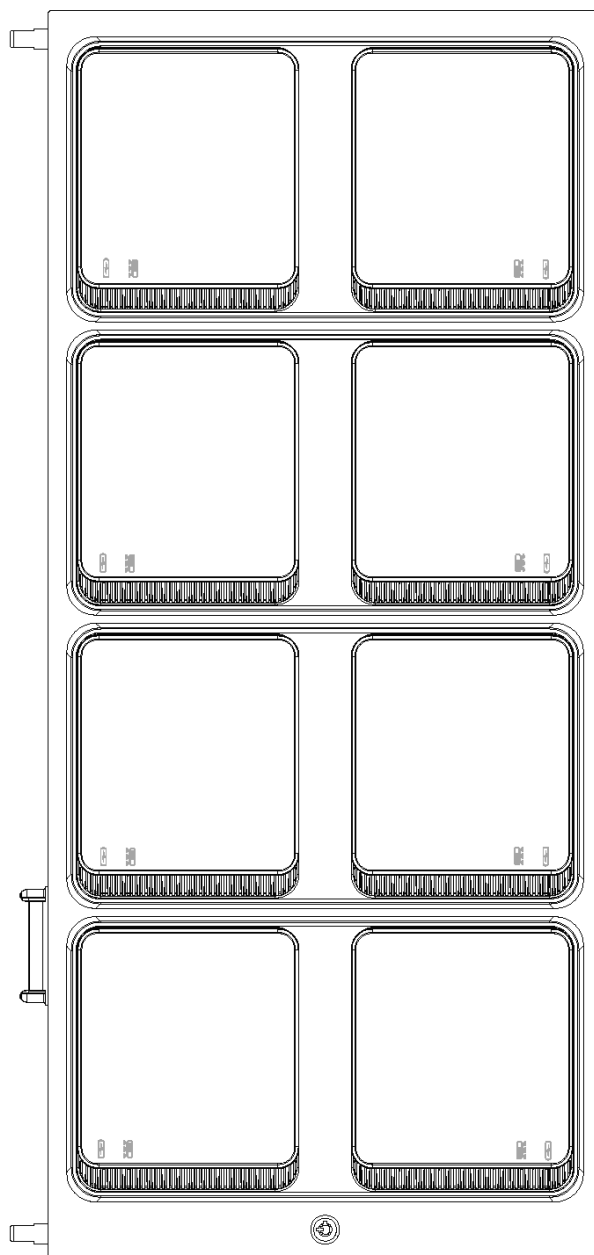
Table 1-1 Appearance description

No.	Name	Description
1	Touch screen	13.3-inch touch screen.
2	Speaker	Audio output.
3	Fingerprint sensor	Add 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	<ul style="list-style-type: none"> 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.

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

1.4 Description of Buttons

Figure 1-4 Ports

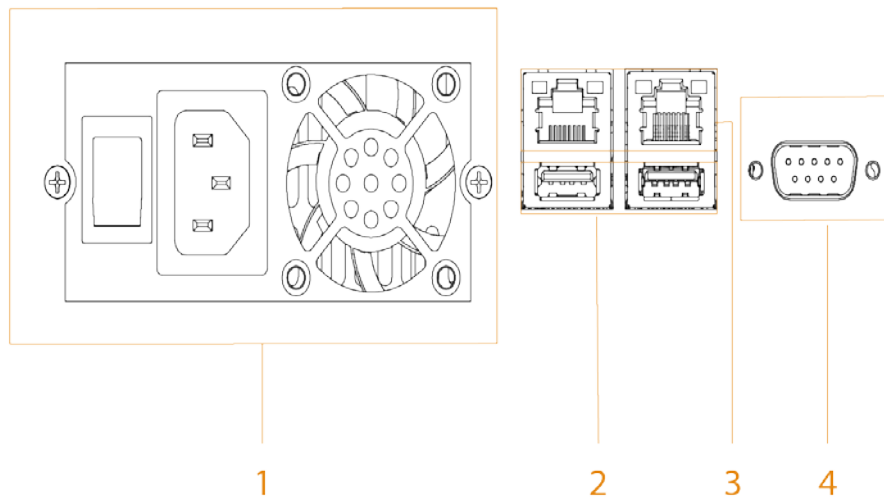




Table 1-2 Port description

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.

1.5 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.

2 Device Connection

2.1 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.

2.2 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 designed exclusively for MPT220 body camera by default. If you want to use them 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 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 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 2-4.

Figure 2-5 Data collection (MPT220 slot)



Figure 2-6 Data collection (MPT210 slot)



3 HDD Installation

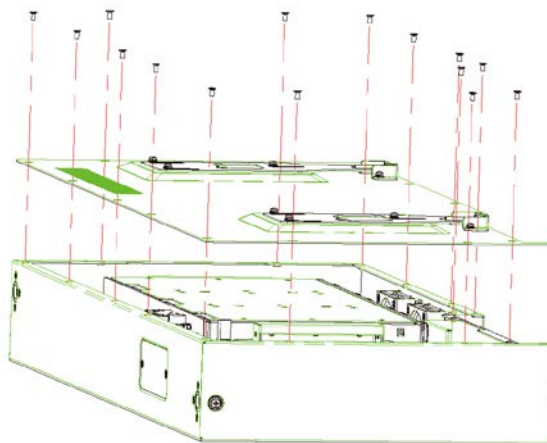
You can install six 10T HDDs (hard disk drives).



- 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.

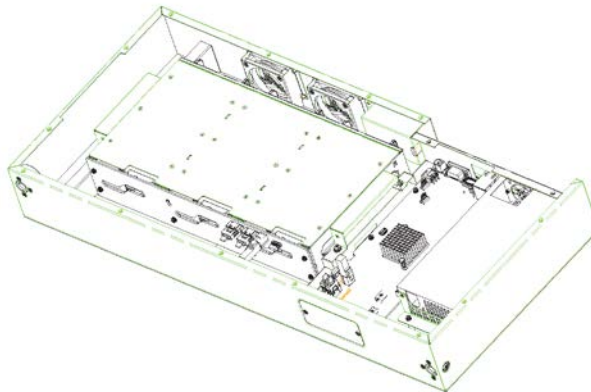
Step 1 Loosen the screws on the rear cover, and then remove the rear cover.

Figure 3-1 Remove rear cover



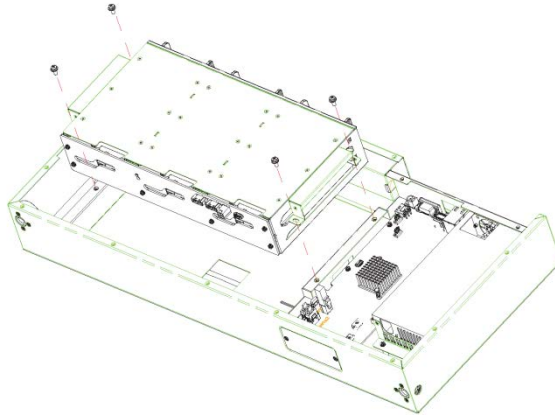
Step 2 Disconnect the cables between main board and HDD plate.

Figure 3-2 Loosen cable



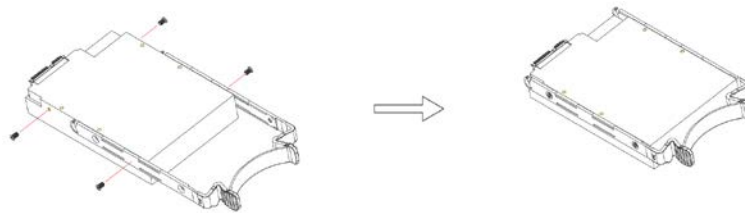
Step 3 Loosen the four fixed screws on the HDD box, and then take out the box.

Figure 3-3 Take out HDD box



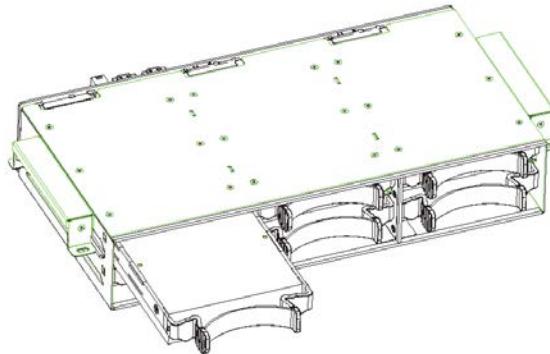
Step 4 Fix HDDs.

Figure 3-4 Fix HDD



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

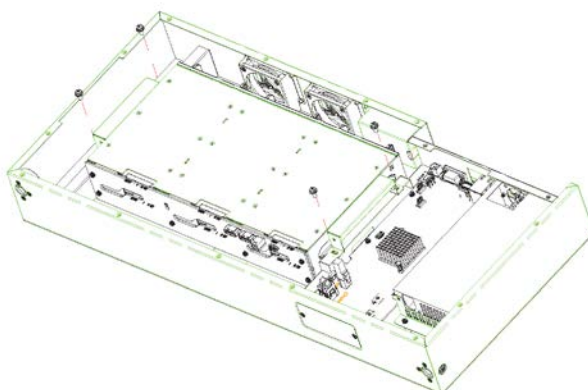
Figure 3-5 Install HDD



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

Step 6 Fix the HDD box in the chassis.

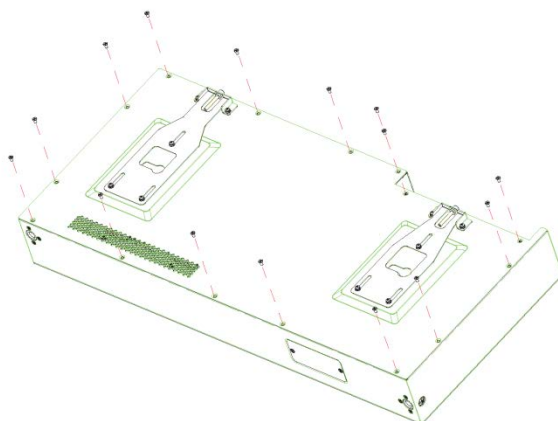
Figure 3-6 Install HDD box



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 Main interface

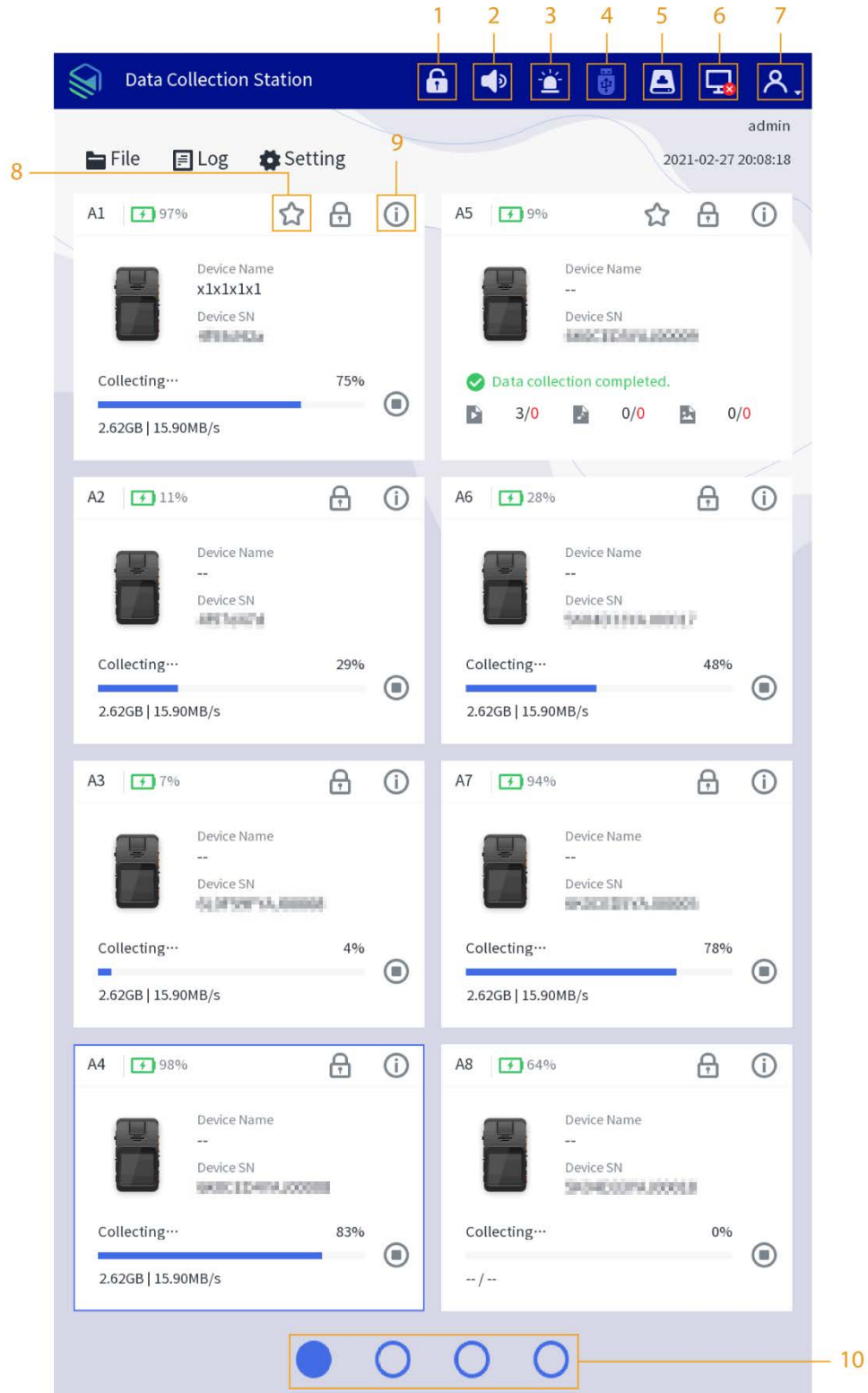







Table 4-1 Main interface description

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.
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.

4.1.1 File Management

4.1.1.1 File Collection

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

4.1.1.2 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, and end time.



The maximum time range for file searching is 1 month.

Figure 4-2 Searching for files

<input type="checkbox"/>	Name	Size	Upload Time	Case No.
<input type="checkbox"/>	20210227195832.dav	373.14 MB	2021-02-27 19:58:32	
<input type="checkbox"/>	20210227195800.dav	184.16 MB	2021-02-27 19:58:00	

4.1.1.3 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.



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

4.1.2 Searching for Log

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

4.1.2.1 Local Log

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



The maximum time range for log searching is 1 month.

Figure 4-3 Local log

No.	Type	Time	Details
1	MPT Operation	2021-02-27 20:11:10	
2	MPT Operation	2021-02-27 20:10:57	

4.1.2.2 Device Log

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



The maximum time range for log searching is 1 month.

Figure 4-4 Device log

No.	Type	Time	Details
1	System	2021-02-27 20:05:19	
2	System	2021-02-27 20:04:55	

4.1.2.3 Collection Log

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



The maximum time range for log searching is 1 month.

Figure 4-5 Collection log

No.	Results	Time	Details
1	Succeed	2021-02-27 20:11:10	
2	Succeed	2021-02-27 20:10:49	

4.1.2.4 Upload Log

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



The maximum time range for log searching is 1 month.

Figure 4-6 Upload log

No.	Results	Time	Details
-----	---------	------	---------

4.1.3 Local Settings

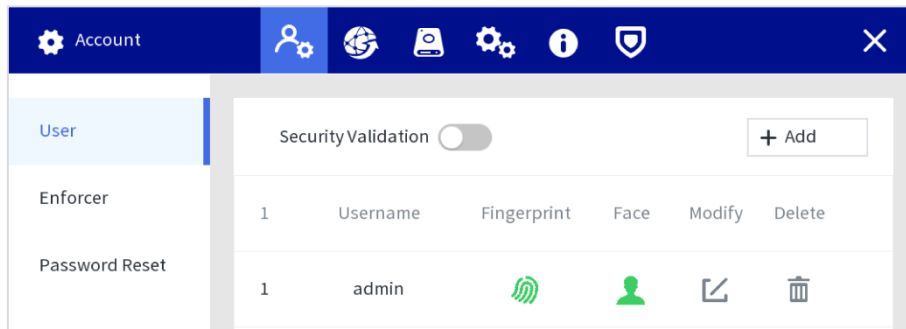
4.1.3.1 User

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

4.1.3.1.1 User Management

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

Figure 4-7 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 4-8 Add users

4.1.3.1.2 Enforcer Management

Select **Setting > Account > Enforcer**.

Adding Enforcer

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

Figure 4-9 Adding enforcer

Add

Enforcer Dept

Enforcer No

Enforcer Name

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

Fingerprint

Searching for Enforcer

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

Figure 4-10 Searching for enforcer

1	Enforcer	Fingerprint Face	Dept	Modify	Delete	Device
1	1					

4.1.3.1.3 Resetting Password

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

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 question after successful setting, click **Reset** first.

Step 3 Click **Apply**.

Figure 4-11 Resetting password

Account

User

Enforcer

Password Reset

Password Reset

Enable ☒

Reserved Email

Security Question

Set successfully. Please reset first if you need to modify securi

Question 1

Answer

Question 2

Answer

Question 3

Answer

Apply

Back

4.1.3.2 Network Management

4.1.3.2.1 TCP/IP

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.

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

Step 2 Configure Ethernet card parameter.


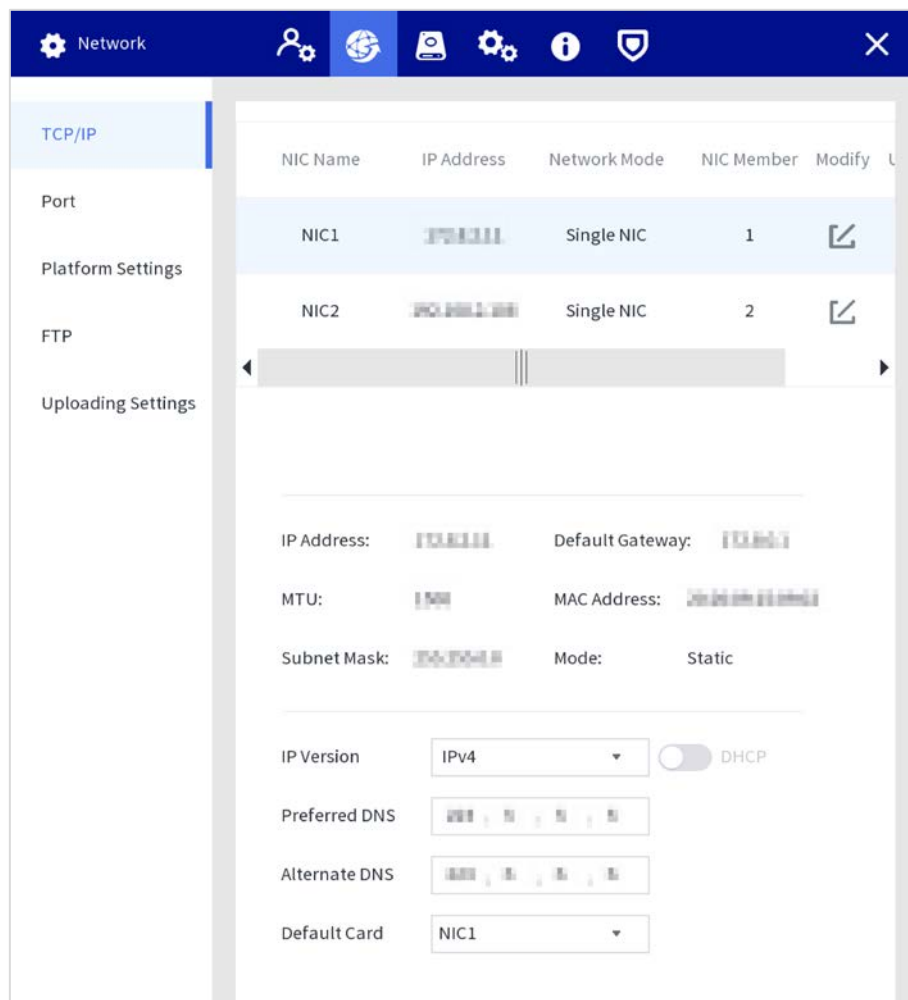


- 1) Click  of the corresponding Ethernet card.
- 2) Configure Ethernet card parameter.

Figure 4-12 IP configuration



The screenshot displays the 'Network' settings window with the 'TCP/IP' tab selected. On the left, a sidebar lists 'Port', 'Platform Settings', 'FTP', and 'Uploading Settings'. The main area features a table of network interfaces:

NIC Name	IP Address	Network Mode	NIC Member	Modify
NIC1	192.168.1.1	Single NIC	1	
NIC2	192.168.1.2	Single NIC	2	

Below the table, configuration fields are shown for the selected NIC (NIC1):

- IP Address: 192.168.1.1
- Default Gateway: 192.168.1.1
- MTU: 1500
- MAC Address: 08:00:27:00:00:00
- Subnet Mask: 255.255.255.0
- Mode: Static
- IP Version: IPv4 (dropdown)
- DHCP: ☐
- Preferred DNS: 192.168.1.1
- Alternate DNS: 192.168.1.1
- Default Card: NIC1 (dropdown)

Step 3 Click **Apply**.

4.1.3.2.2 Port

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

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

Step 2 Configure port parameter.

Figure 4-13 Configure port parameter

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)

Table 4-2 Port parameters description

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

Parameter	Description
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.

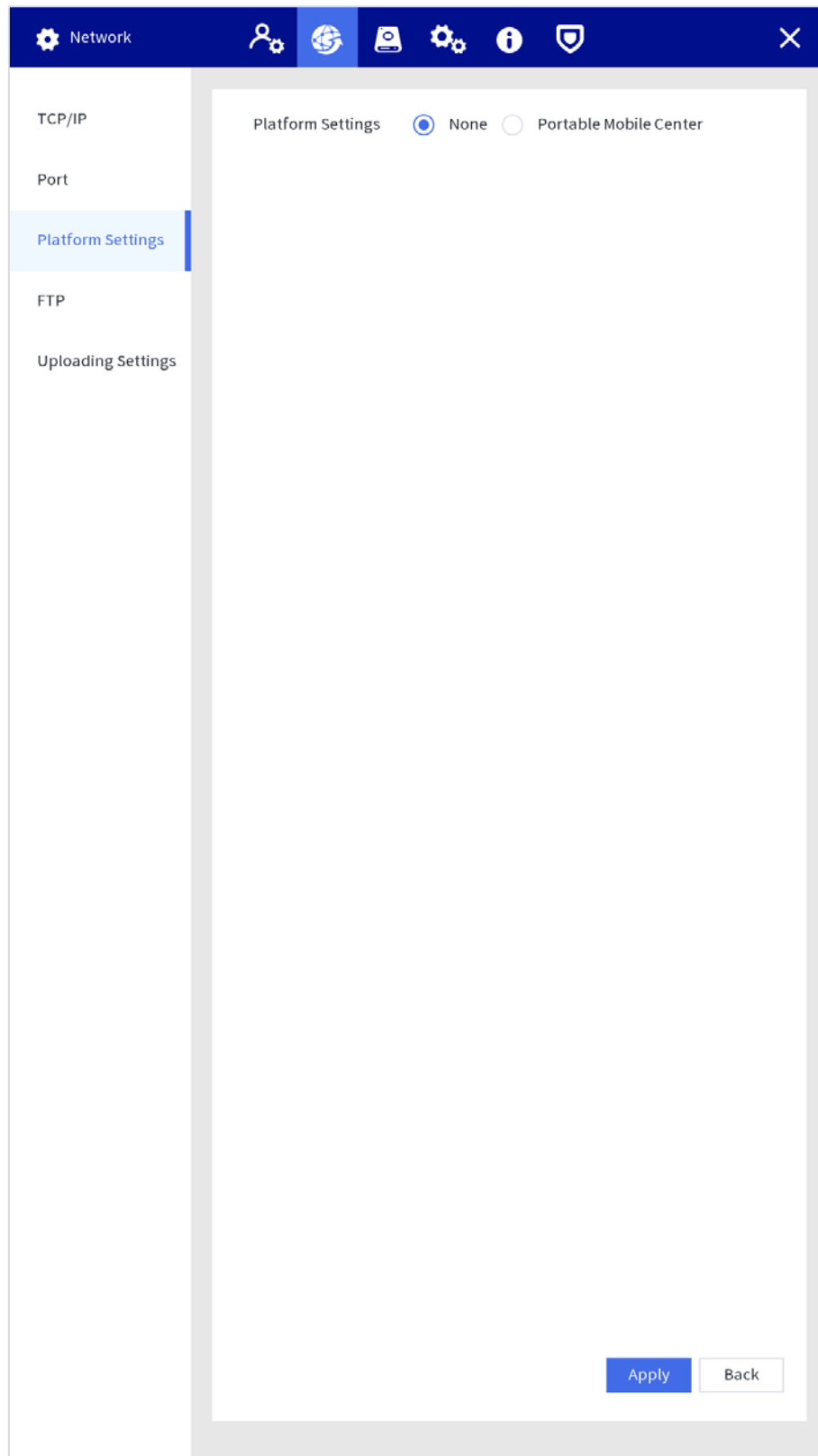
Step 3 Click **Apply**.

4.1.3.2.3 Platform Settings

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

Step 2 Select **None** or **Portable Mobile Center** as needed.

Figure 4-14 Platform settings



Step 3 Click **Apply**.

4.1.3.2.4 FTP Setting

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 4-15 FTP setting

The screenshot displays the 'FTP' settings page within a network management application. The interface includes a top navigation bar with icons for Network, User, Global, Storage, Settings, Info, and Security. A left sidebar contains menu items: TCP/IP, Port, Platform Settings, FTP (highlighted), and Uploading Settings. The main area shows the FTP configuration: 'Enable' is a toggle switch turned on; 'Type' has radio buttons for 'FTP' and 'SFTP (Recommended)' (selected); 'Server Address' is an empty text field; 'Port' is a text field with '22' and a range '(1 - 65535)'; 'Username' is a text field with 'admin'; 'Password' is a masked text field with 6 dots; 'Storage Path' is an empty text field; 'Character Encode' is a dropdown menu set to 'UTF-8'. At the bottom are 'Test', 'Apply', and 'Back' buttons.

Table 4-3 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

Parameter	Description
Username	The username and password for logging in to the FTP server.
Password	
Storage Path	<p>The destination path in the FTP server.</p>  <p>Create folder on FTP server.</p> <ul style="list-style-type: none"> If you do not enter the name of remote directory, 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	<p>Supports UTF-8 and GB2312.</p>  <p>When messy codes are displayed on the server, switch the character encode.</p>

Step 3 Click **Apply**.

4.1.3.3 Storage Management

You can manage the storage resources (such as record file) and storage space. So that it is easy for you to use and enhance storage space usage.

4.1.3.3.1 Basic

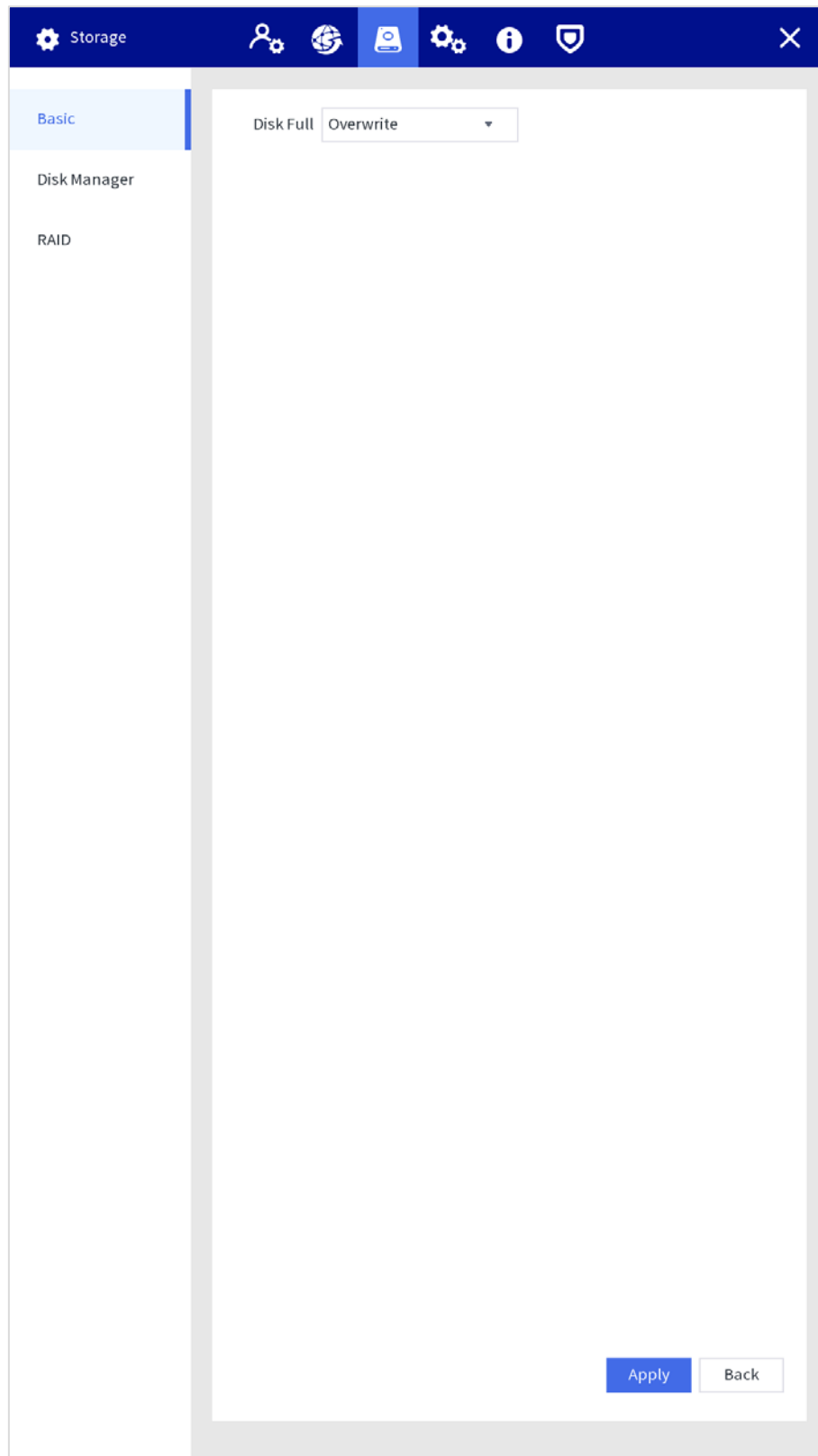
Step 1 Select **Setting > Storage > Basic**.

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.

Figure 4-16 Basic configuration



Step 3 Click **Apply**.

4.1.3.3.2 Disk Manager

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

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

Step 2 Click  to view the details.

Step 3 (Optional) Format an HDD.

- 1) Select an HDD and then click **Format**.
- 2) Click **OK**.
- 3) Enter the admin password and click **OK**.
All data in the HDD is deleted.



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

[illegible]

4.1.3.3.3 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 RAID0, RAID1, RAID5, RAID10. For details, see "Appendix 1 Raid Introduction." This section takes RAID 5 as an example.
- We recommend deploying RAID disk at the beginning of RAID configuration. Creating or deleting RAID will affect device data.

Configuring RAID

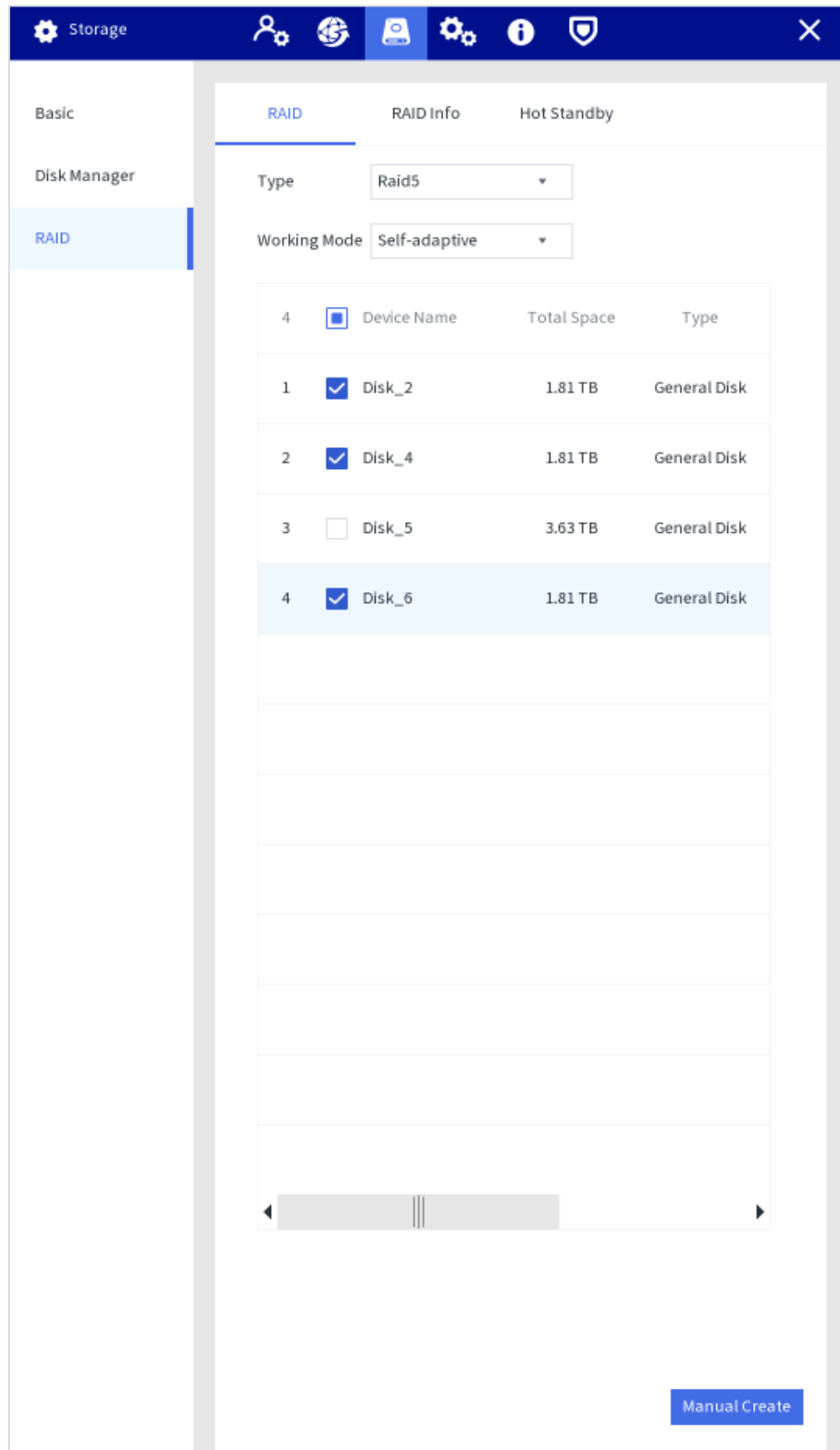
Step 1 Select **Setting > Storage > RAID > RAID**.

Step 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 4-18 RAID



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

Step 4 Click **Manual Create**.

Step 5 Click **Confirm**.

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

Figure 4-19 Create RAID successfully

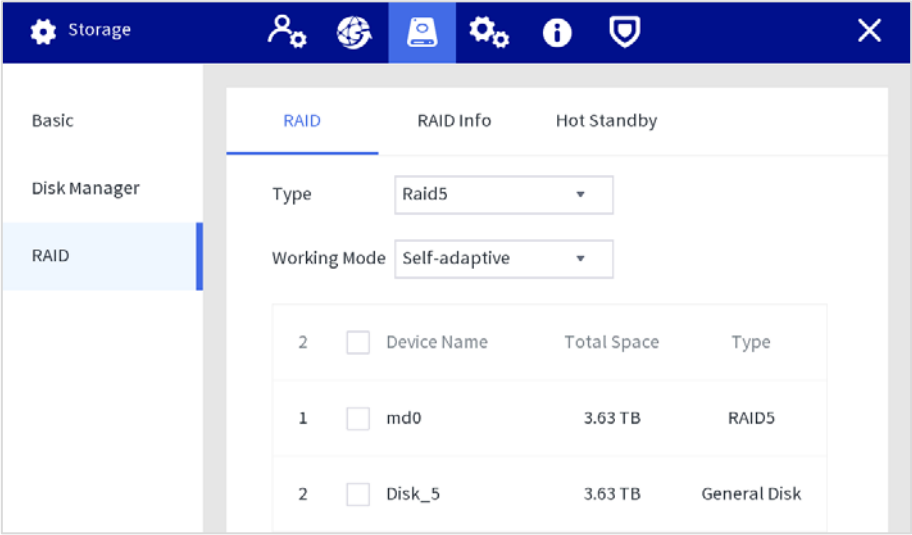


Figure 4-20 Display in disk manager RAID is created (1)

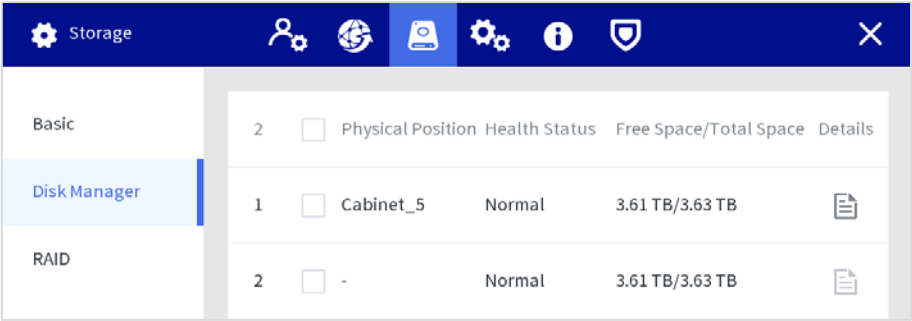
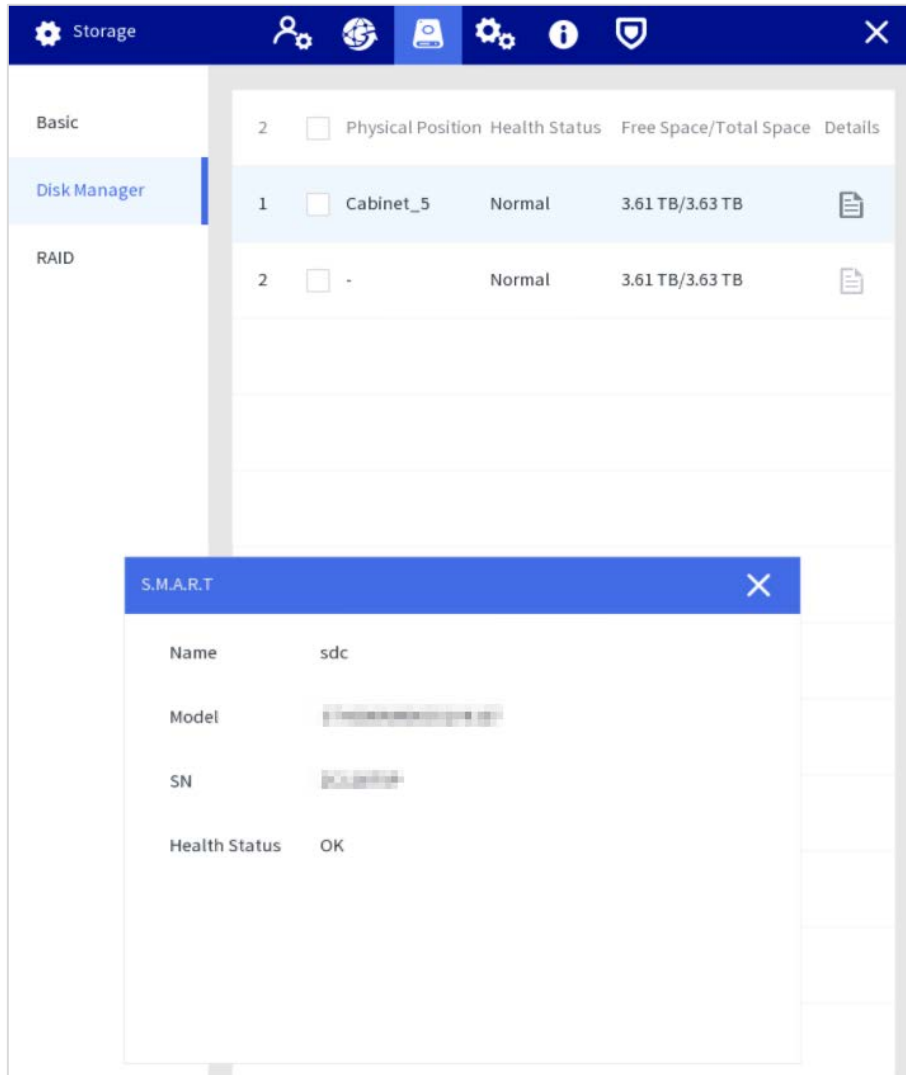


Figure 4-21 Display in disk manager RAID is created (2)



RAID Information

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

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

Figure 4-22 RAID information

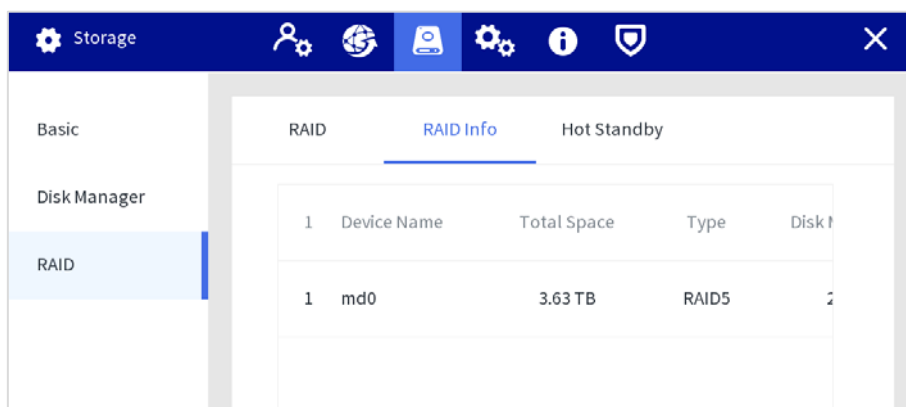


Figure 4-23 Details

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

	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.

Step 1 Select **Setting > Storage > RAID > Hot Standby**.

Step 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.

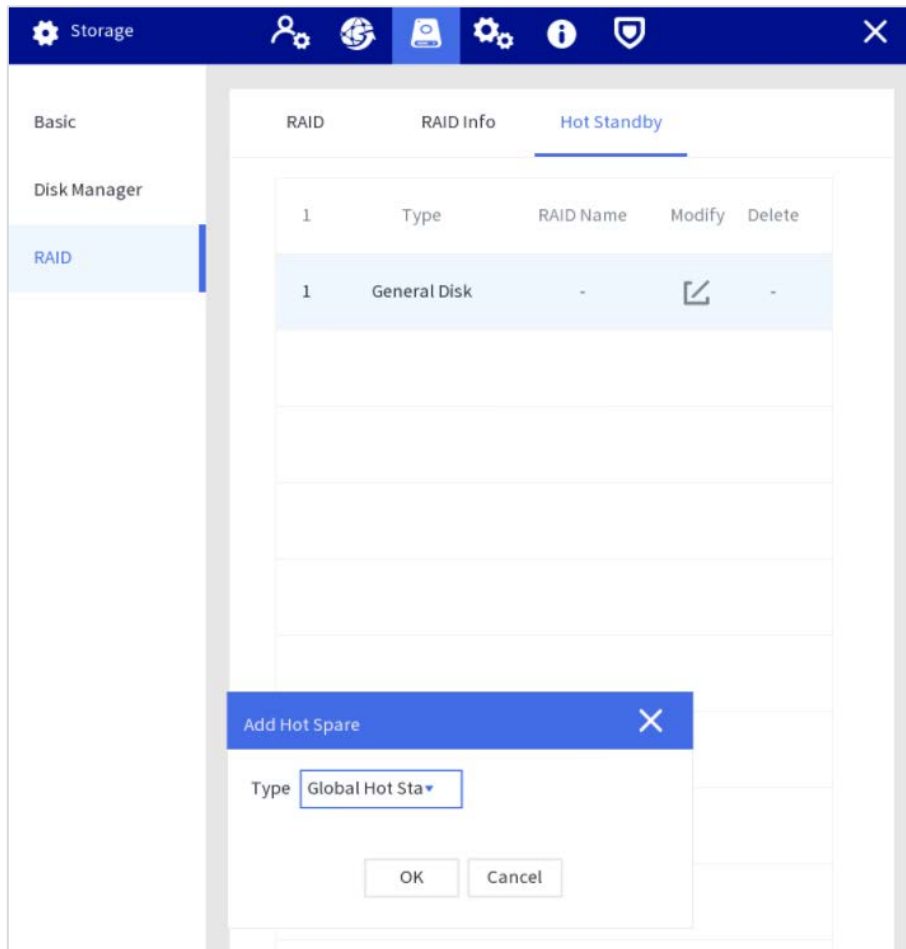
The screenshot shows the 'Storage' configuration window. On the left, the 'RAID' tab is selected under 'Disk Manager'. The main area displays the 'RAID' configuration page with three tabs: 'RAID', 'RAID Info', and 'Hot Standby'. The 'RAID' tab is active, showing a table with one RAID configuration:

1	Type	RAID Name	Modify	Delete
1	General Disk	-	[edit icon]	-

Below the table, an 'Add Hot Spare' modal dialog is open. It contains the following fields:

- Type: Private Hot Sp
- Add to: md0
- Buttons: OK, Cancel

Figure 4-25 Global hot standby



Step 3 Click **OK**.

After authentication, the hot standby is created successfully.

Figure 4-26 Global hot standby

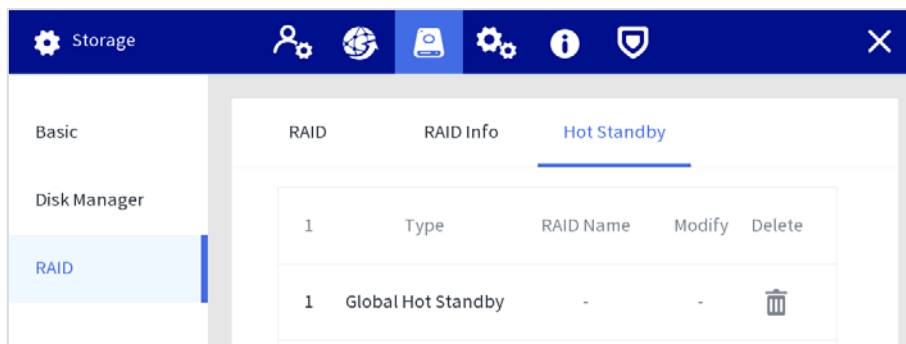
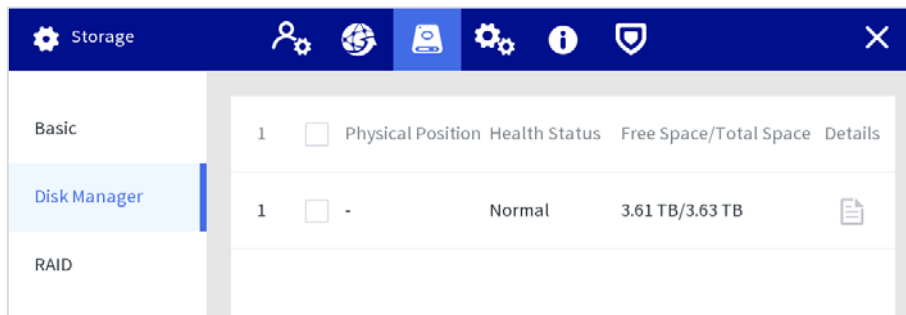


Figure 4-27 Display in disk manager after hot standby is created



4.1.3.4 System Management

4.1.3.4.1 Basic Setting

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

Figure 4-28 Basic setting

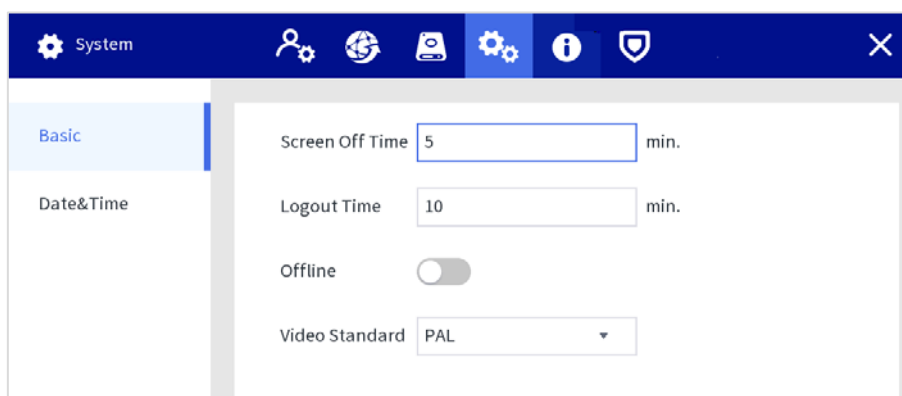



Table 4-4 Date and time parameters

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 extending 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.

4.1.3.4.2 Date and Time

Step 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 4-29 Date and time

The screenshot displays the 'Date and time' configuration window. The interface includes a top navigation bar with icons for System, User, Network, Storage, Settings (highlighted), Info, and Security. A left sidebar contains 'Basic' and 'Date&Time' tabs, with 'Date&Time' being the active tab. The main content area is divided into sections for manual time setting and NTP (Network Time Protocol) configuration. The manual time section includes fields for System Time (2021-02-27 20:21:15), Time Zone ((UTC+08:00) Beijing, C), Date Format (YYYY MM DD), Date Separator (-), and Time Format (24-Hour). The DST (Daylight Saving Time) section has a toggle switch turned off, with options for Date and Week. The NTP section has a toggle switch turned off, with fields for Server Address (time.windows.com), Port (123), and Interval (60 min.). A 'Manual Update' button is also present. At the bottom right, there are 'Apply' and 'Back' buttons.

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)

[Apply] [Back]

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

Table 4-5 Date and time parameters

Parameter	Description
System Time	Set the device system date and time. Click Sync PC to synchronize time with the PC from where you log in to the web interface.
Time Zone	Time zone of the current area.
Date Format	Select a date format from YYY MM DD , MM DD YYY , and DD MM YYY .
Date Separator	Select a separator between year, month, and date.
Time Format	Select a time format from 24-Hour and 12-Hour .
DST	When you enable DST, 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.

- 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.

Step 2 Click **Apply**.

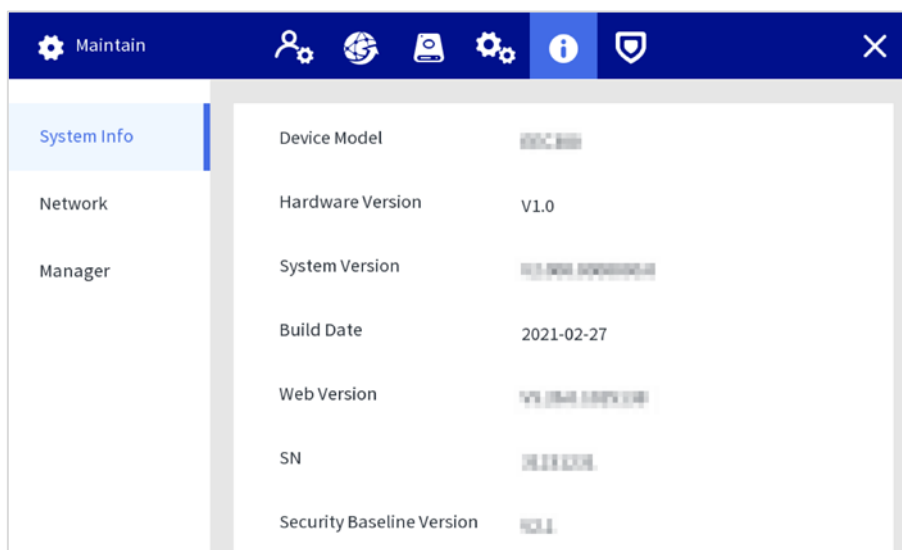
4.1.3.5 Operation & Maintenance Management

4.1.3.5.1 System Information

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

Select **Setting > Maintain > System Info**.

Figure 4-30 System information



4.1.3.5.2 Network

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

Figure 4-31 Network information

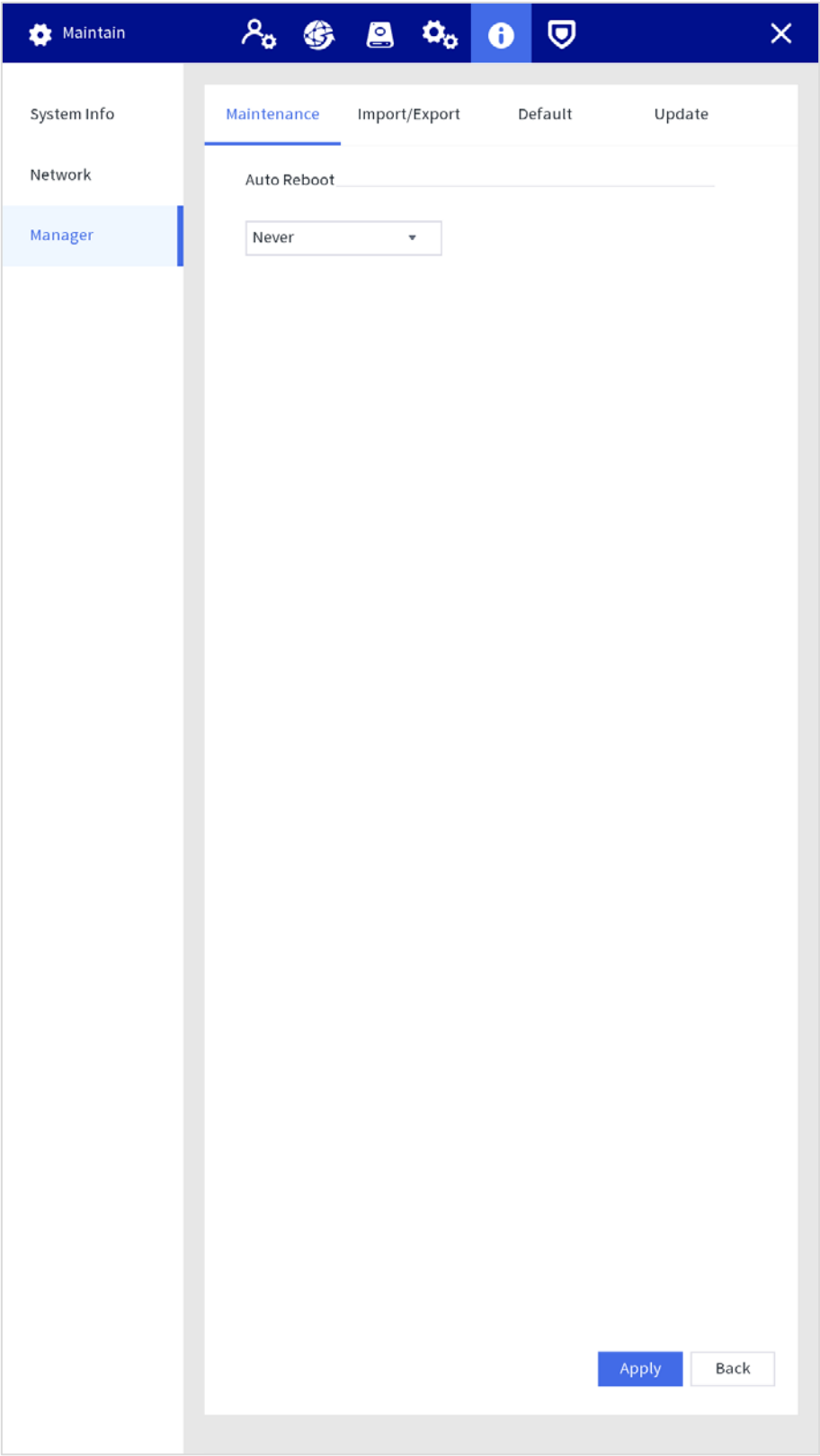
[illegible]

4.1.3.5.3 Maintain

Device Maintain

Step 1 Select **Setting > Maintain > Manager > Maintenance**, and then set the maintenance date.

Figure 4-32 Device maintenance



Step 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.

Step 1 Select **Setting > Maintain > Manager > Import/Export**.

Step 2 Select **Export** from the **Operation Type** list, select the file type and storage path as needed, and then enter the password.

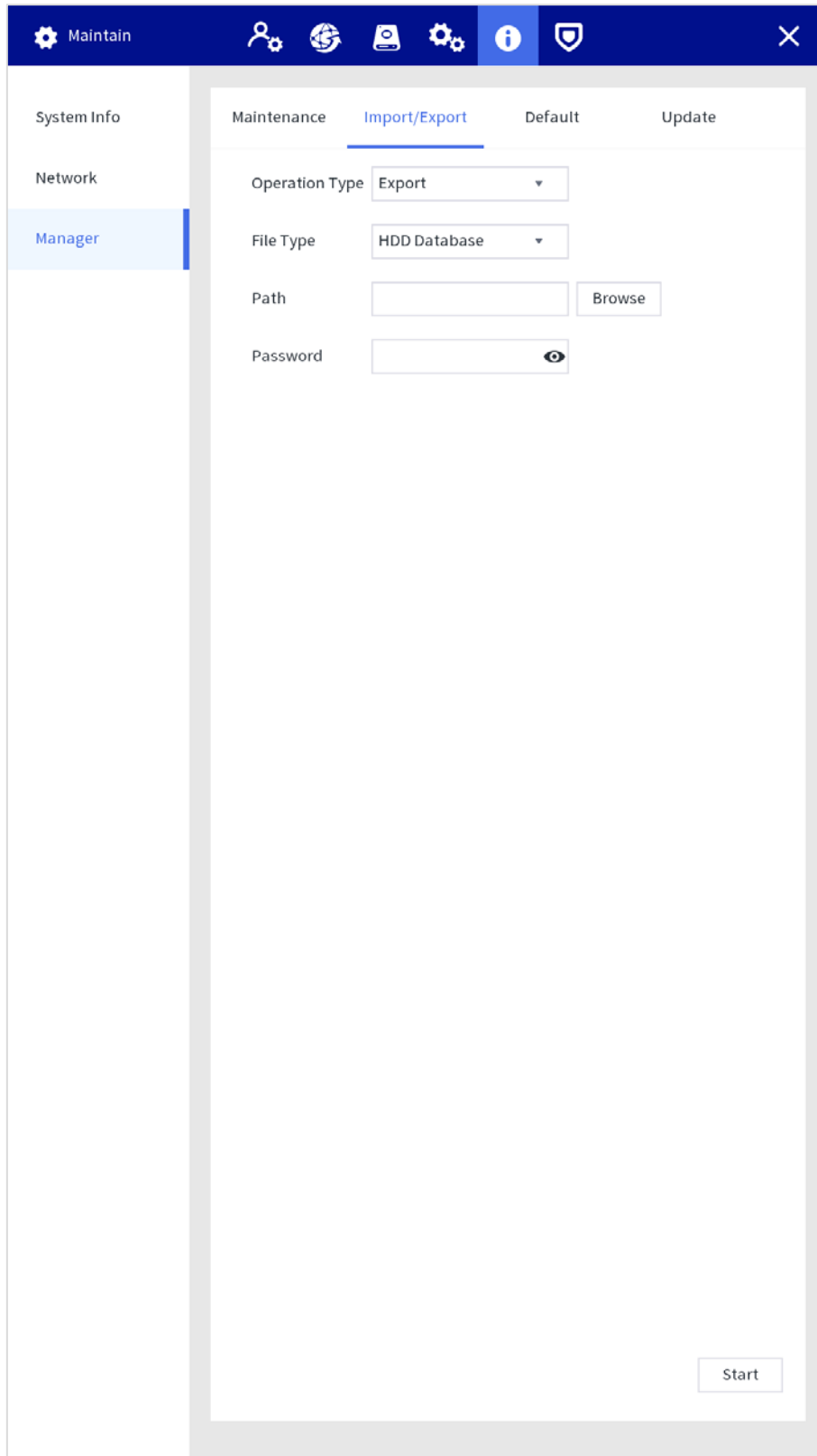
Step 3 Click **Start**.

Step 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.

Step 5 Click **Start**.

Import configuration file, and then restart the Station.

Figure 4-33 Export configuration



The image shows a web-based configuration interface for exporting data. At the top, there is a dark blue header bar with a 'Maintain' button and several icons. On the left, a sidebar contains 'System Info', 'Network', and 'Manager' (which is highlighted). The main content area has tabs for 'Maintenance', 'Import/Export' (selected), 'Default', and 'Update'. Under the 'Import/Export' tab, there are four fields: 'Operation Type' (set to 'Export'), 'File Type' (set to 'HDD Database'), 'Path' (with a 'Browse' button), and 'Password' (with a toggle icon). A 'Start' button is located at the bottom right of the configuration area.

Maintain

System Info

Network

Manager

Maintenance Import/Export Default Update

Operation Type Export

File Type HDD Database

Path Browse

Password

Start

Figure 4-34 Import configuration

The screenshot shows a software application window titled "Import configuration". The window has a dark blue header bar with a "Maintain" button and several icons. On the left, there is a sidebar with "System Info", "Network", and "Manager" (which is highlighted). The main area has four tabs: "Maintenance", "Import/Export" (which is active), "Default", and "Update". Under the "Import/Export" tab, there are four fields: "Operation Type" (set to "Import"), "File Type" (set to "User"), "Path" (with a "Browse" button), and "Password" (with a toggle icon). A "Start" button is located at the bottom right of the main area.

Maintenance	Import/Export	Default	Update
Operation Type <input type="text" value="Import"/>			
File Type <input type="text" value="User"/>			
Path <input type="text"/> <input type="button" value="Browse"/>			
Password <input type="text"/> <input type="button" value="toggle"/>			
<input type="button" value="Start"/>			

Default

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

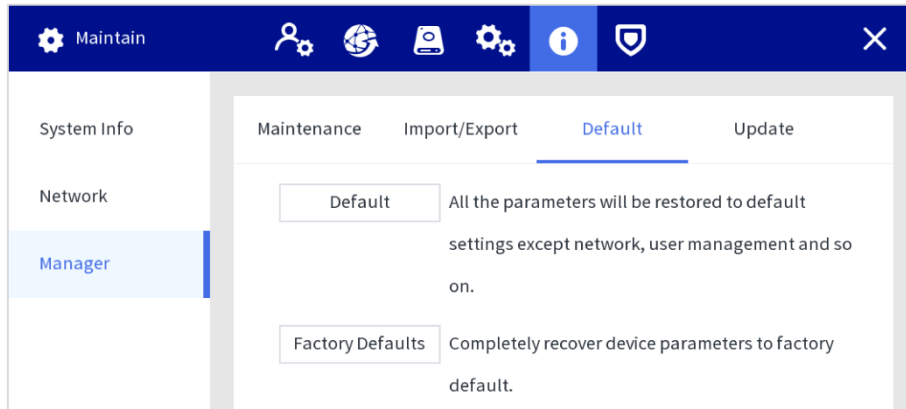


Click **Factory Defaults**, all configurations except the data in the external storage will be deleted. You can delete data in an external storage by formatting the storage media and other methods.

Step 1 Select **Setting > Maintain > Manager > Default**.

Step 2 Click **Default** or **Factory Defaults** as needed.

Figure 4-35 Default



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

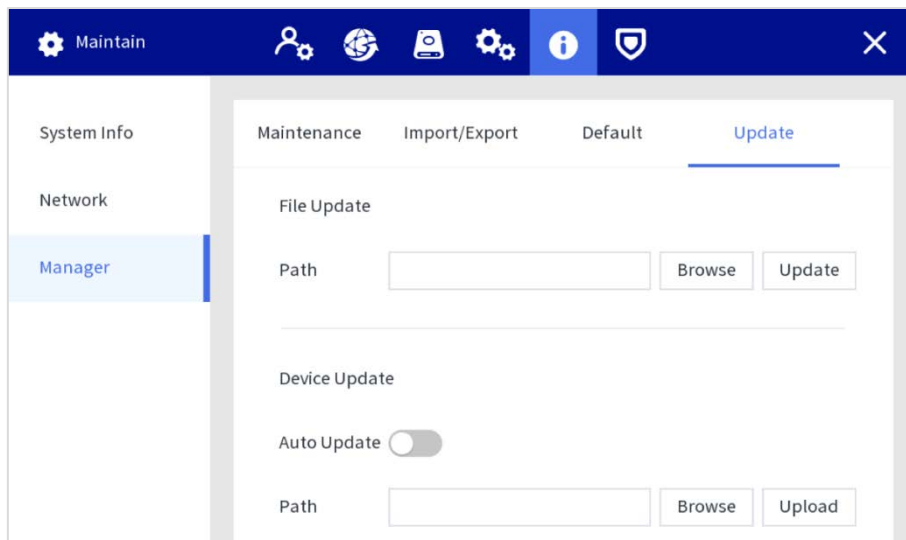
Station Update

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.

Step 1 Select **Setting > Maintain > Manager > Update**.

Step 2 Select the update file, and then click **Update**.

Figure 4-36 Update




Body Camera 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 click **Upload** to upload the file of latest version. Click  on the main interface, and then click the **Update** tab to update the device.

4.1.3.6 Security

4.1.3.6.1 Security Status

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

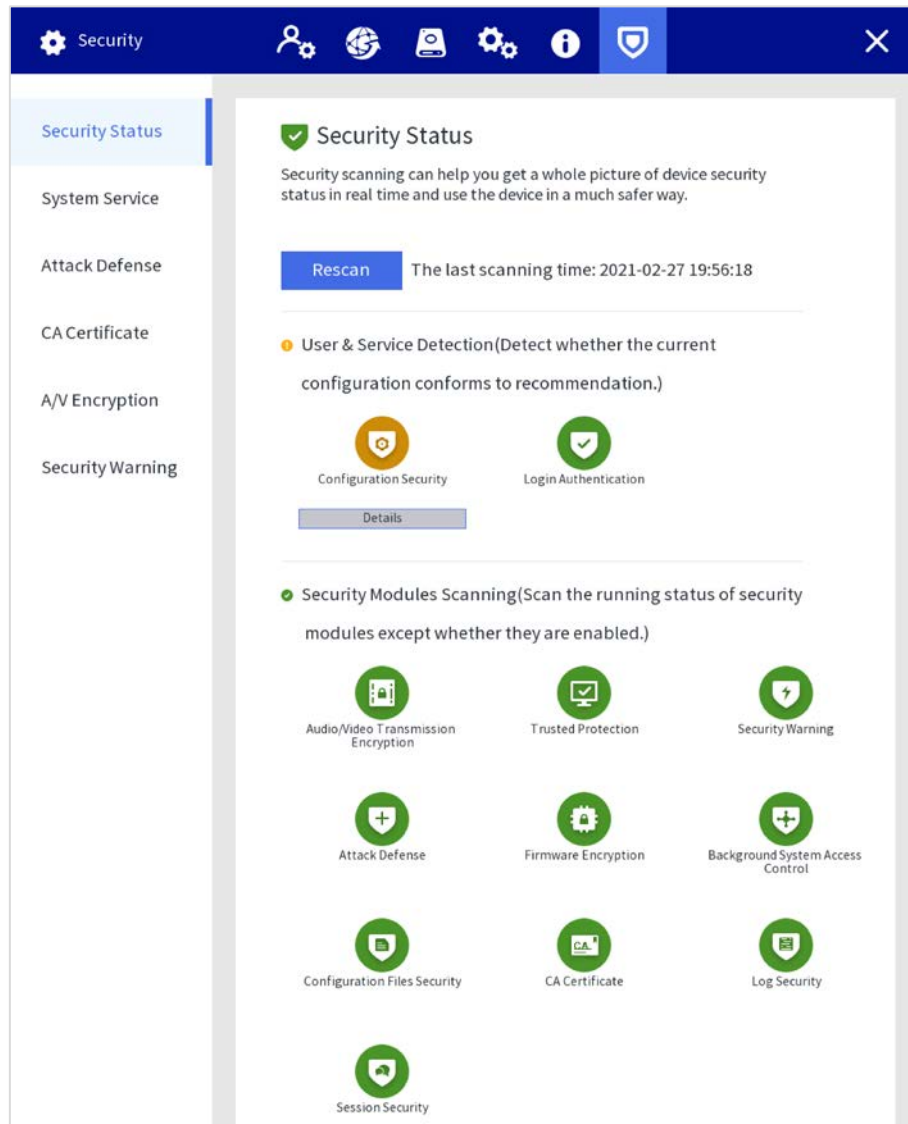
- **User and service detection:** Detect login authentication, user status, and configuration security to check whether the current configuration conforms to recommendation.
- **Security modules scanning:** Scan the running status of security modules, such as audio/video transmission, trusted protection,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

Procedure

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

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

Figure 4-37 Security status



Results

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

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

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



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

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

4.1.3.6.2 System

Basic Service

Step 1 Select **Setting > Security > System Service > Basic Services**.

Step 2 Configure parameters.

Figure 4-38 Basic services

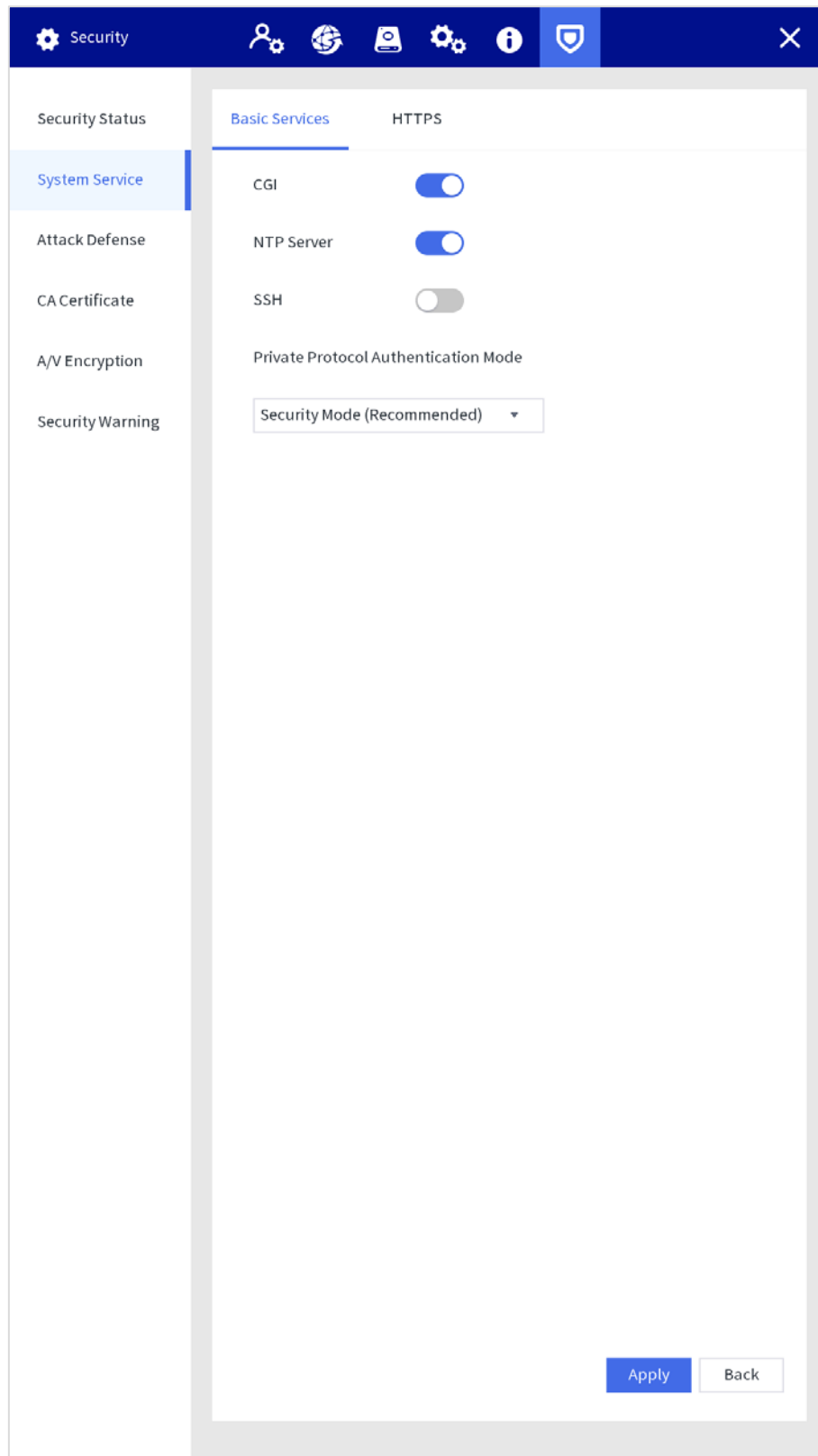


Table 4-6 Basic service parameters description

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.

Parameter	Description
SSH	You can enable SSH authentication to realize safety management. It is enabled by default.
Private Protocol Authentication Mode	Select private protocol authentication mode to guarantee the device security when login. Security Mode is recommended.

Step 3 Click **Apply**.

HTTPS

Through creating server certificate, the PC 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 to HTTPS service. If the service is disabled, there might be risk of data leakage.

Procedure

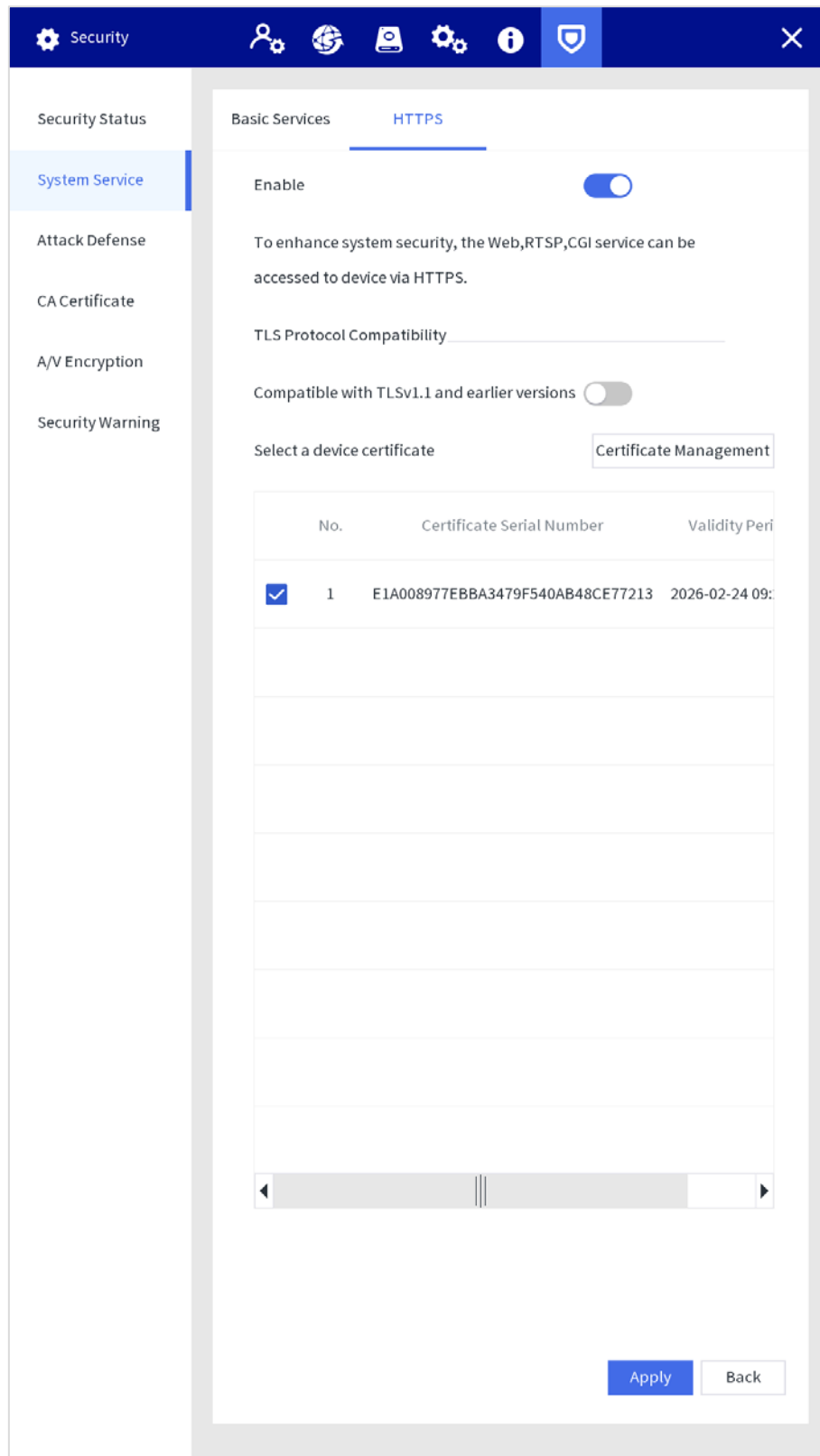
Step 1 Select **Setting > Security > Security Center > HTTPS**.

Step 2 Enable HTTPS, and then select the certification.



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

Figure 4-39 HTTPS



Step 3 (Optional) Click ☐ next to **Compatible with TLSv1.1 and earlier versions** to enable the protocol compatibility function.

Step 4 Click **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`.

4.1.3.6.3 Attack Defense

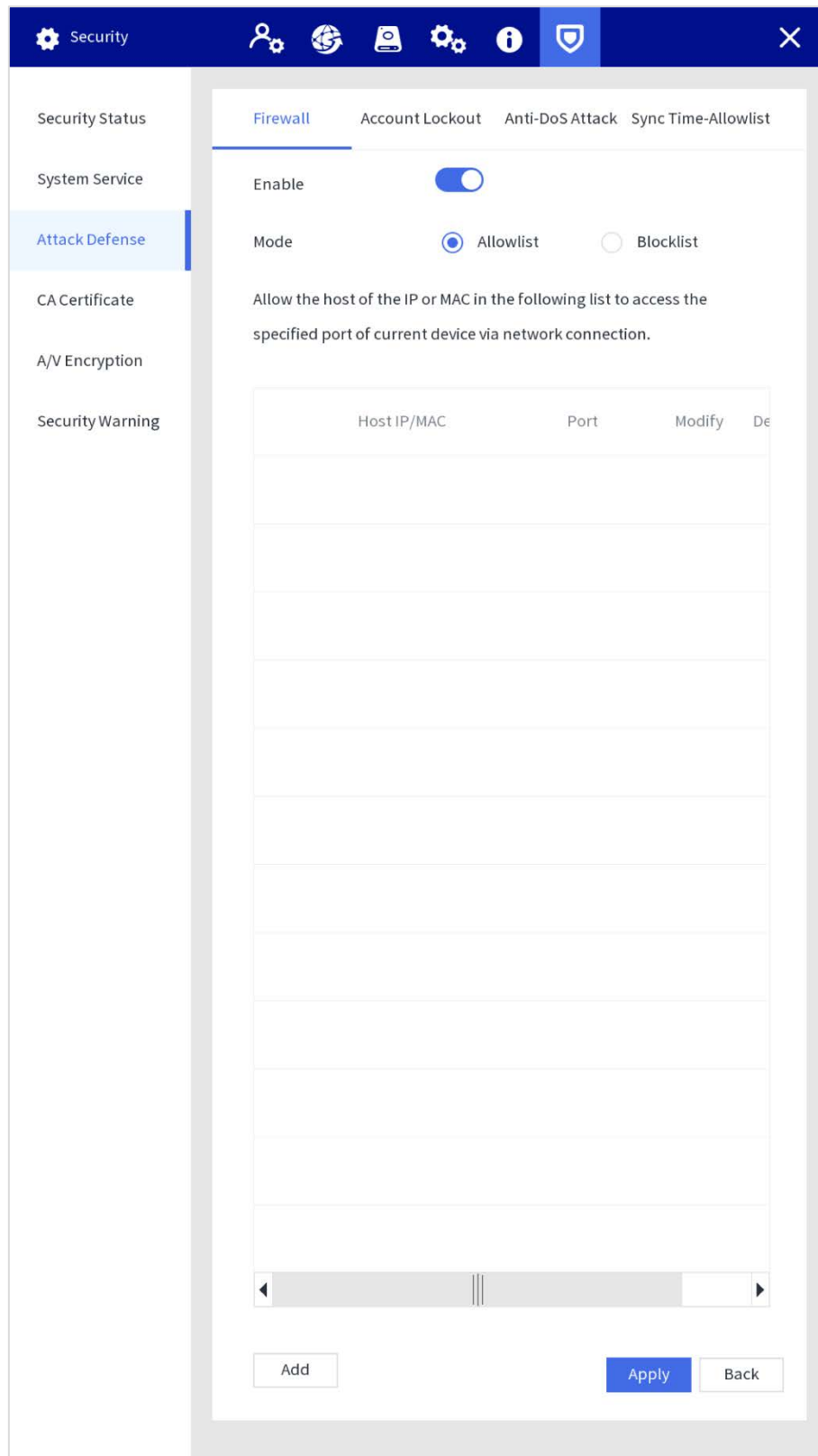
Firewall

Configure firewall to limit access to the Station.

Step 1 Select **Setting > Security > Attack Defense > Firewall**.

Step 2 Enable the firewall function.

Figure 4-40 Firewall



Step 3 Select the access mode.

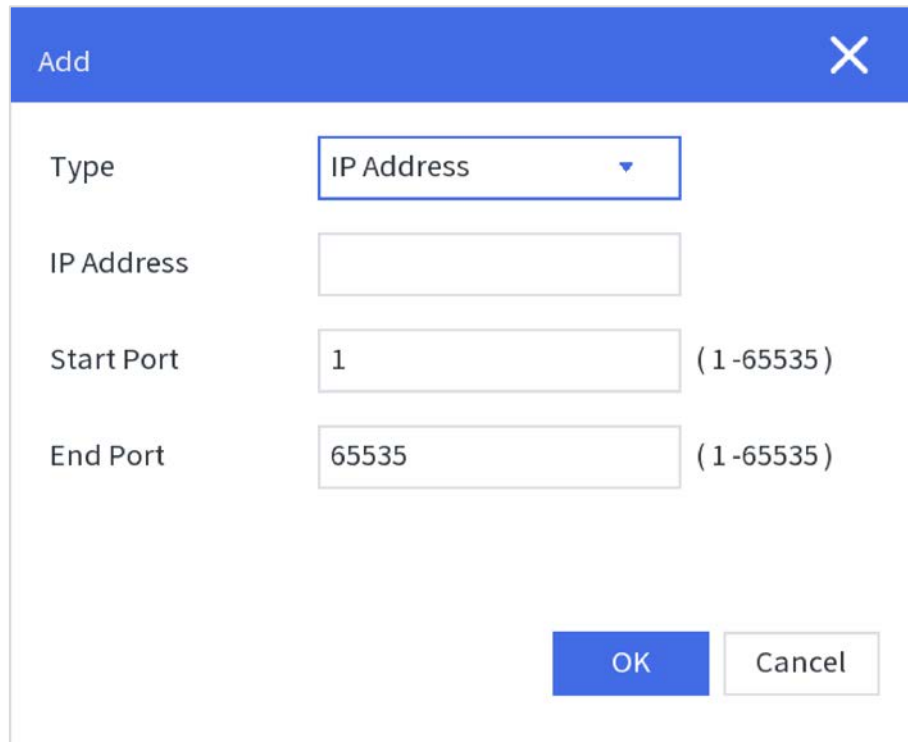
Allowlist and Blocklist cannot be enabled at same time.

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

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

- 1) Click **Add**.
- 2) Enter the information of IP host as needed.

Figure 4-41 Add allowlist

A dialog box titled "Add" with a blue header bar containing a close button (X). The dialog contains four input fields: "Type" with a dropdown menu showing "IP Address", "IP Address" with an empty text box, "Start Port" with a text box containing "1" and a range "(1 -65535)" to its right, and "End Port" with a text box containing "65535" and a range "(1 -65535)" to its right. At the bottom right are "OK" and "Cancel" buttons.

Type	IP Address
IP Address	
Start Port	1 (1 -65535)
End Port	65535 (1 -65535)

OK Cancel

3) Click **OK**.

Step 5 Click **Apply**.

Account Lockout

If you consecutively enter a wrong password more than the configured value, the account will be locked.

Step 1 Select **Setting > Security > Attack Defense > Account Lockout**.

Step 2 Configure parameters.

- **Login Attempt:** Upper limit of login attempts. If you consecutively enter a wrong password more than the configured value, the account will be locked.
- **Lock Time:** The period during which you cannot log in after the login attempts reach upper limit.

Figure 4-42 Account lock

The screenshot shows a web-based security configuration interface. At the top, there is a dark blue header bar with a 'Security' label and several icons. On the left, a vertical sidebar contains a list of security-related options: 'Security Status', 'System Service', 'Attack Defense' (which is highlighted with a blue bar), 'CA Certificate', 'A/V Encryption', and 'Security Warning'. The main content area is titled 'Account Lockout' and contains the following text: 'An account will be temporarily locked after 5 failed login attempts. It cannot log in for 30 minutes.' Below this text, there are two input fields: 'Login Attempt' with the value '5' and 'Lock Time' with the value '30' followed by 'min.'. At the bottom right of the main content area, there are two buttons: 'Apply' (in blue) and 'Back' (in white with a blue border).

Step 3 Click **Apply**.

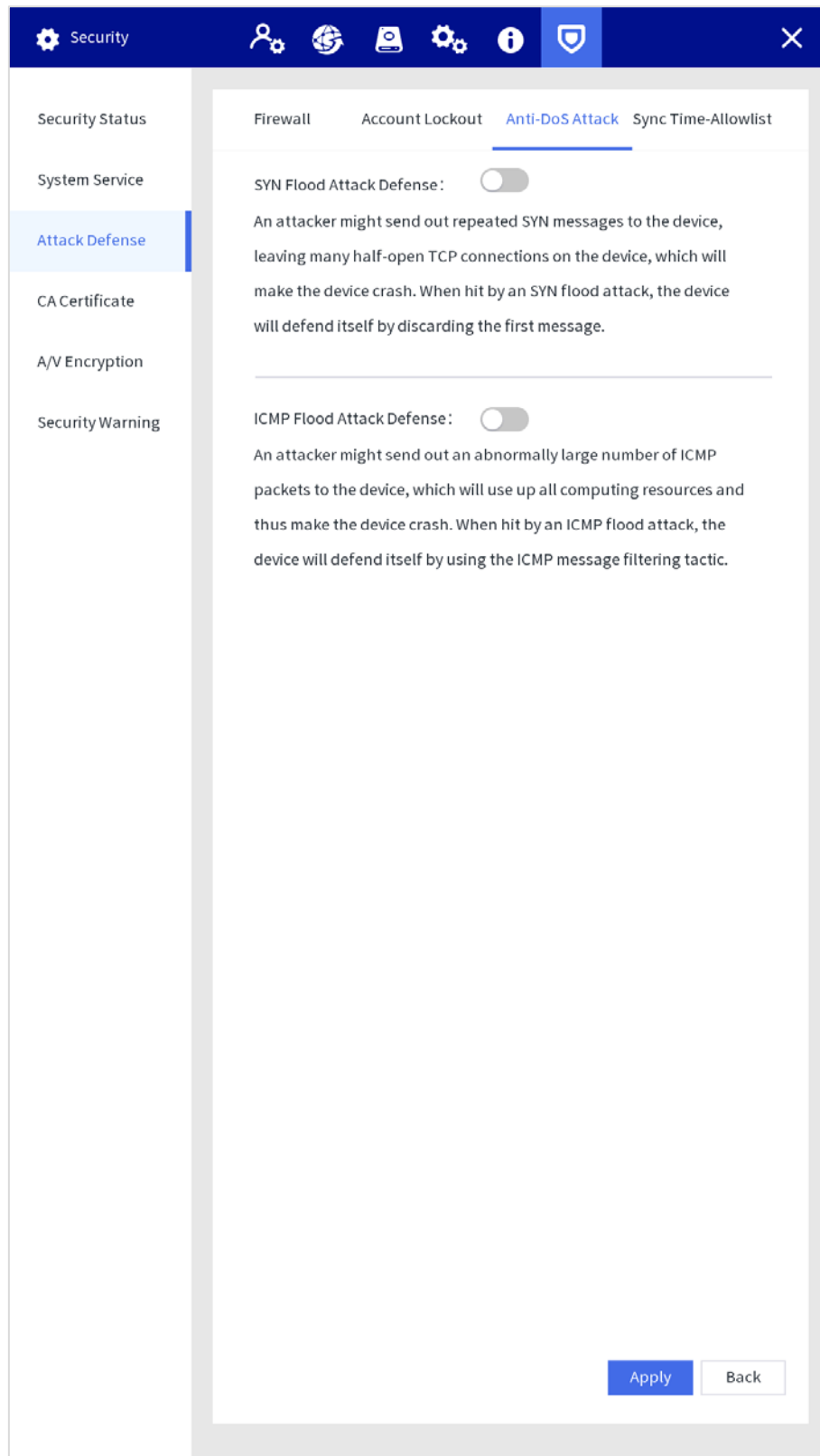
Anti-DoS Attack

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

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

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

Figure 4-43 Anti-DoS attack



Step 3 Click **Apply**.

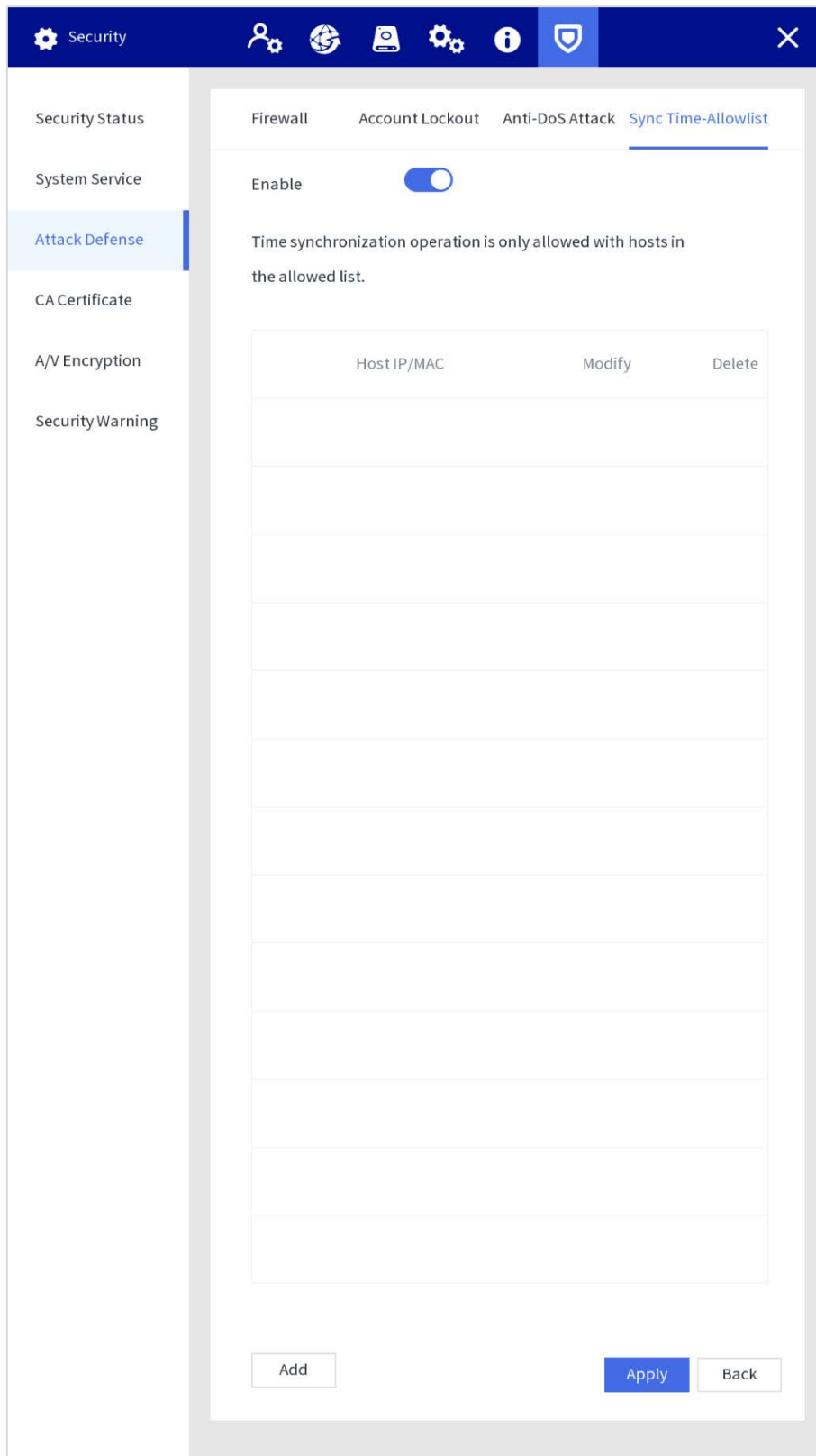
Sync Time-Allowlist

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.

Step 1 Select **Setting > Security > Attack Defense > Sync Time-Allowlist**.

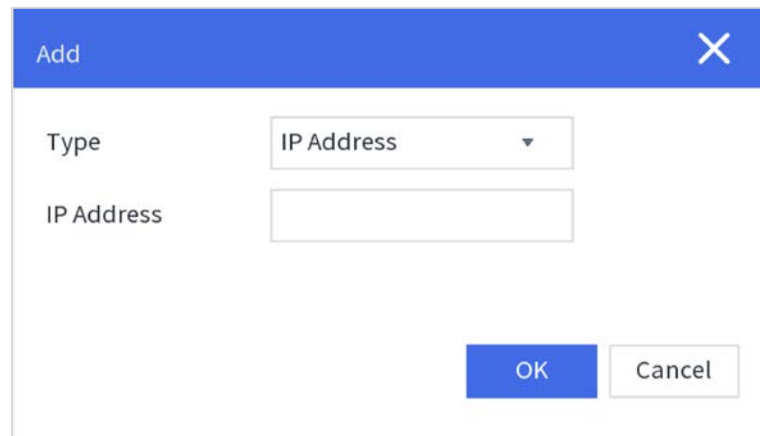
Step 2 Enable the sync time-allowlist function.

Figure 4-44 Sync time-allowlist



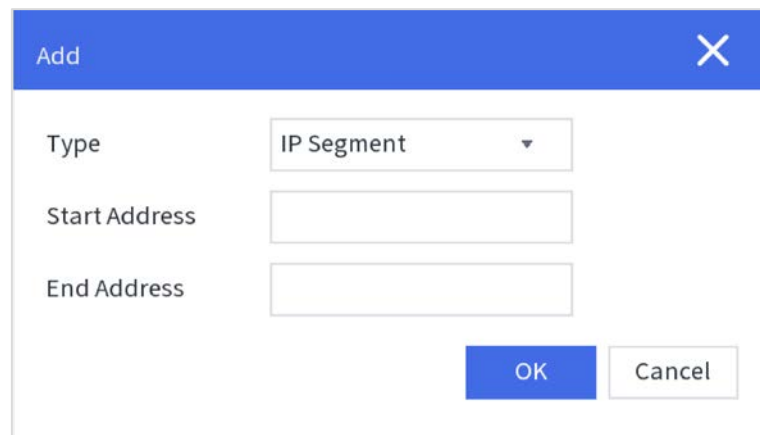
Step 3 Click **Add** to add the IP/MAC of the source host through IP address or IP segment.

Figure 4-45 Add IP address



The dialog box has a blue header bar with the text "Add" on the left and a close button (X) on the right. Below the header, there are two labels: "Type" and "IP Address". The "Type" label is next to a dropdown menu that currently shows "IP Address". The "IP Address" label is next to a text input field. At the bottom right of the dialog, there are two buttons: "OK" (blue) and "Cancel" (white with a blue border).

Figure 4-46 IP segment



The dialog box has a blue header bar with the text "Add" on the left and a close button (X) on the right. Below the header, there are three labels: "Type", "Start Address", and "End Address". The "Type" label is next to a dropdown menu that currently shows "IP Segment". The "Start Address" label is next to a text input field. The "End Address" label is next to a text input field. At the bottom right of the dialog, there are two buttons: "OK" (blue) and "Cancel" (white with a blue border).

Step 4 Click **Apply**.

4.1.3.6.4 CA Certificate

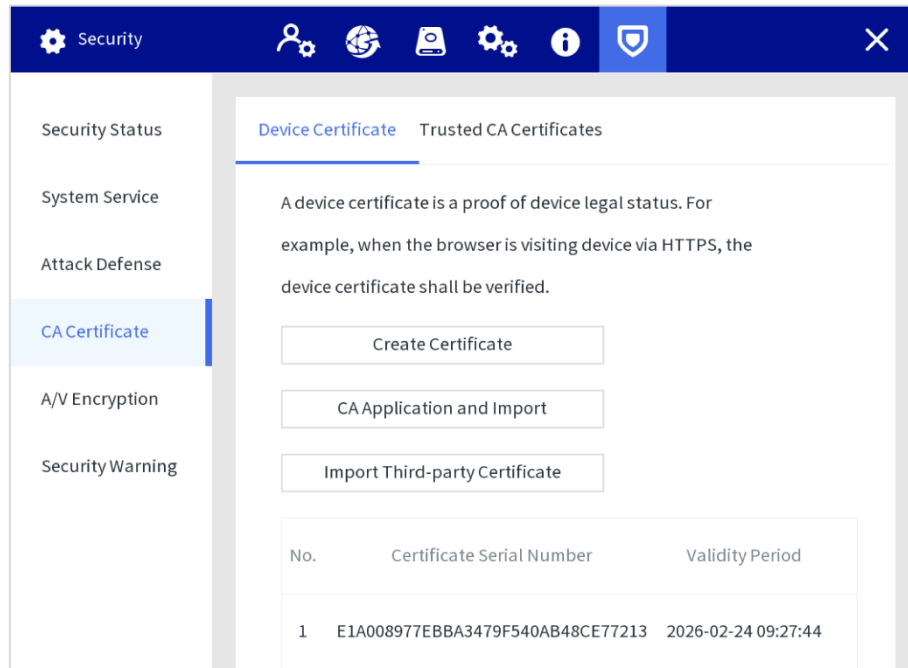
Create a certificate or upload an authenticated certificate, and then you can log in through HTTPS with web browser.

Creating certificate

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

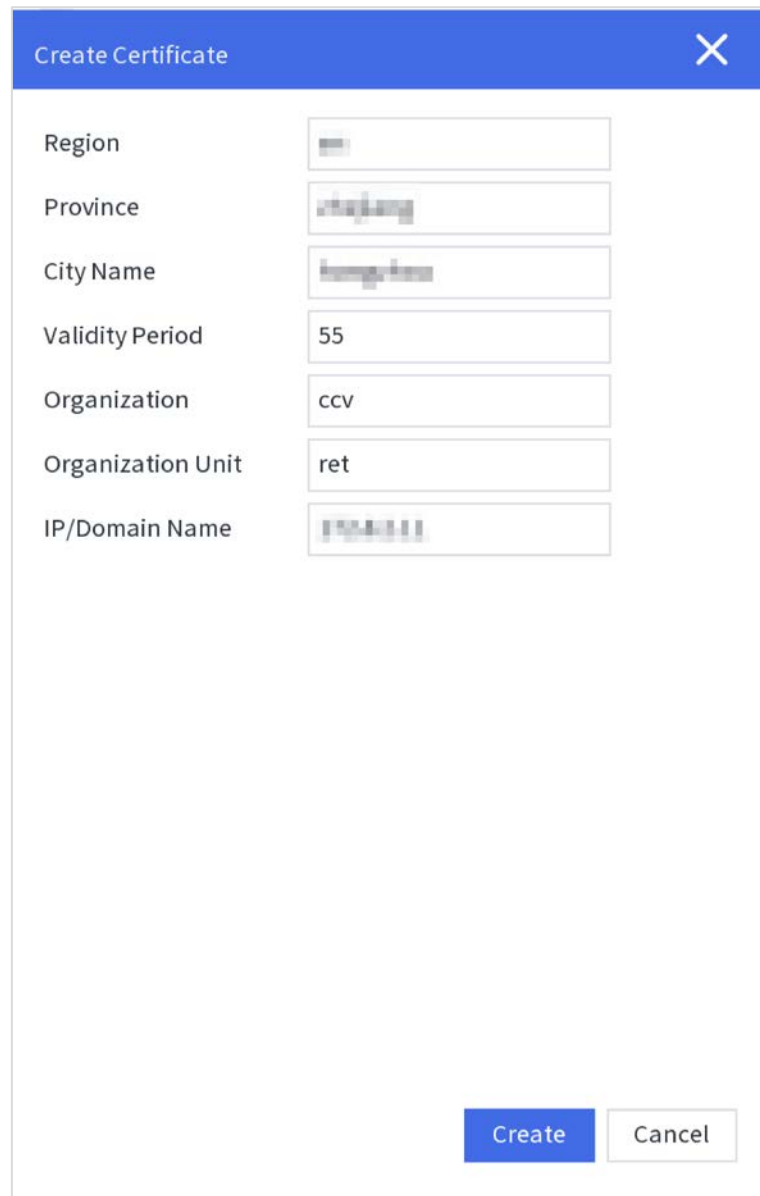
Step 2 Click **Create Certificate**.

Figure 4-47 Device certificate



Step 3 Enter the certificate information as needed.

Figure 4-48 Create certificate



The image shows a 'Create Certificate' dialog box with a blue header bar containing the title and a close button. The main area contains seven input fields for certificate information. At the bottom right, there are 'Create' and 'Cancel' buttons.

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

Step 4 Click **Create**.

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

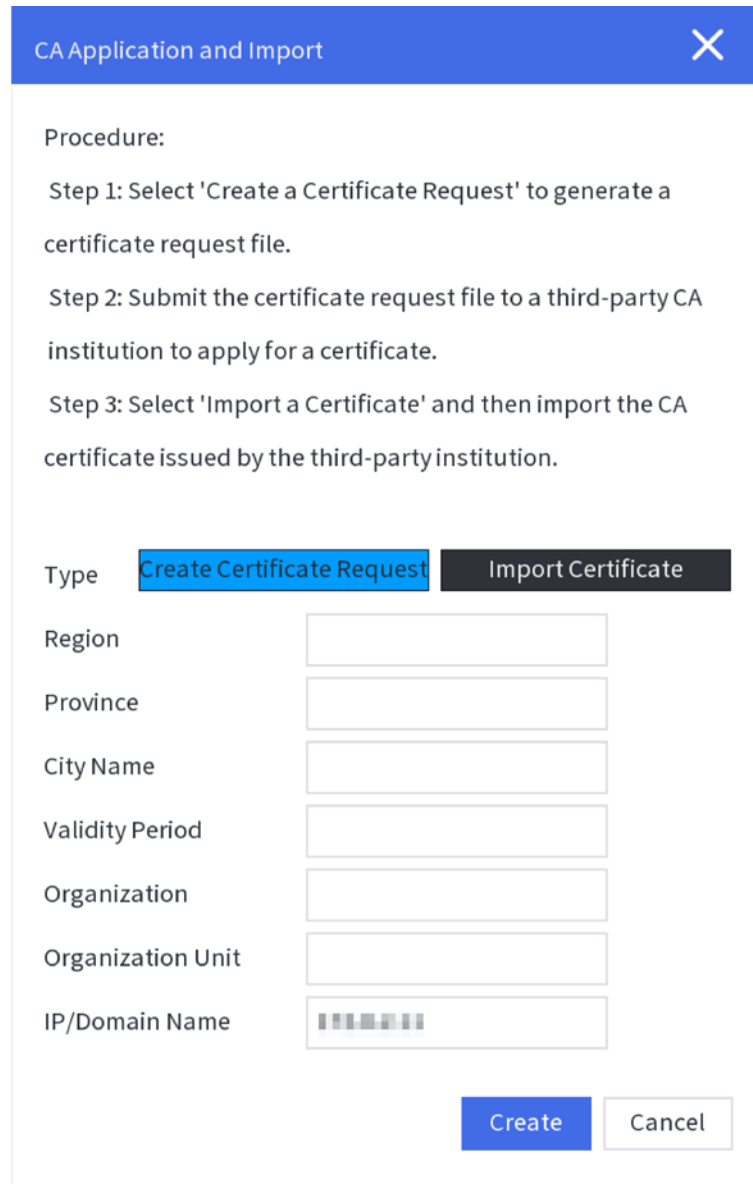
Applying for and Importing CA Certificate

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

Step 2 Click **CA Application and Import**.

Step 3 Enter the certificate information, and click **Create** to save the certificate to an external device.

Figure 4-49 Apply for and importing CA certificate



The image shows a software dialog box titled "CA Application and Import" with a close button (X) in the top right corner. The dialog contains a "Procedure:" section with three steps: 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), and Step 3 (Select 'Import a Certificate' and then import the CA certificate issued by the third-party institution). Below the procedure, there is a "Type" section with two buttons: "Create Certificate Request" (highlighted in blue) and "Import Certificate" (dark grey). Underneath these buttons are several input fields: "Region", "Province", "City Name", "Validity Period", "Organization", "Organization Unit", and "IP/Domain Name". The "IP/Domain Name" field has a small icon of a network card. At the bottom right, there are two buttons: "Create" (blue) and "Cancel" (light grey).

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

Step 4 Apply for the CA certificate from the third-party certificate authority.

Step 5 Import CA certificate.

- 1) Save the CA certificate to a USB flash drive, and then insert the drive to the Station.
- 2) Click **Import Certificate** on the **CA Application and Import** interface.
- 3) Import the certificate according to the screen instruction.

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

Importing Third-party Certificate

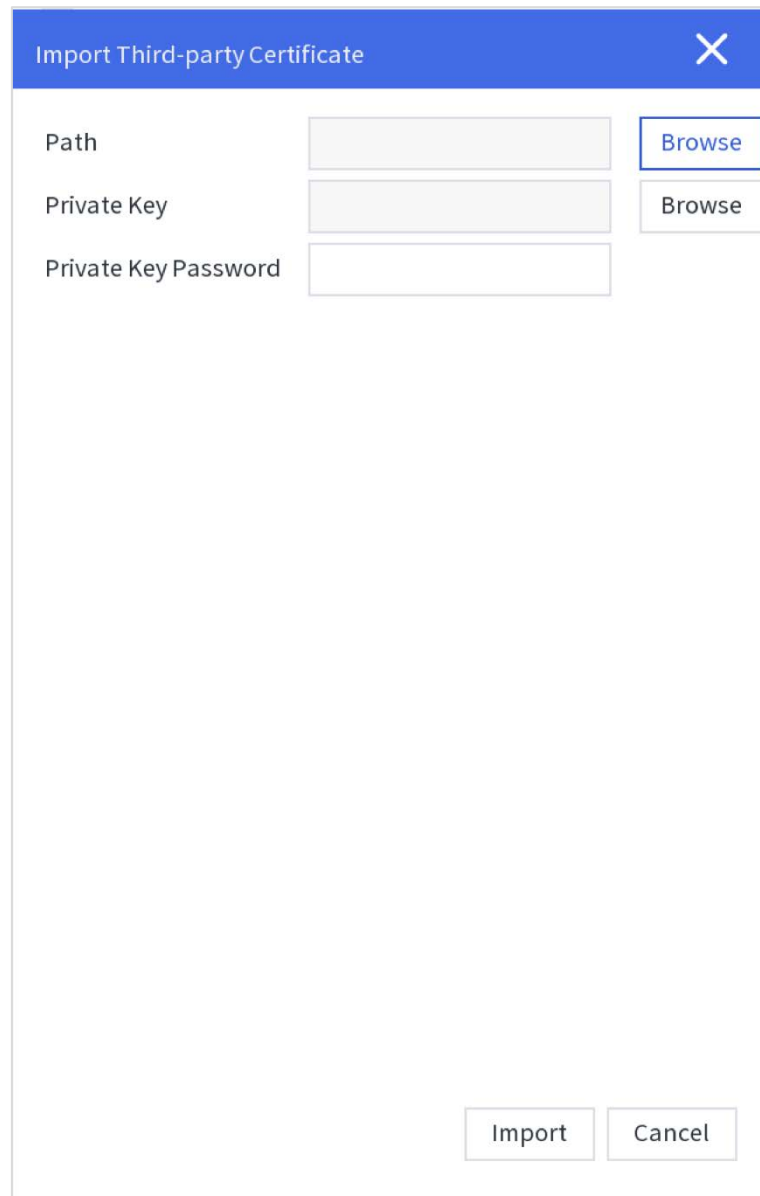
Save the third-party certificate to a USB flash drive, and then insert the drive to the Station.

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

Step 2 Click **Import Third-party Certificate**.

Step 3 Select the certificate and private key file, and enter the private key password.

Figure 4-50 Import third-party certificate



The dialog box titled "Import Third-party Certificate" has a blue header bar with a close button (X) in the top right corner. It contains three input fields: "Path", "Private Key", and "Private Key Password". The "Path" and "Private Key" fields have "Browse" buttons to their right. The "Private Key Password" field is a single-line text input. At the bottom right, there are "Import" and "Cancel" buttons.

Import Third-party Certificate	
Path	<input type="text"/> <input type="button" value="Browse"/>
Private Key	<input type="text"/> <input type="button" value="Browse"/>
Private Key Password	<input type="password"/>
<input type="button" value="Import"/> <input type="button" value="Cancel"/>	

Step 4 Click **Import**.

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

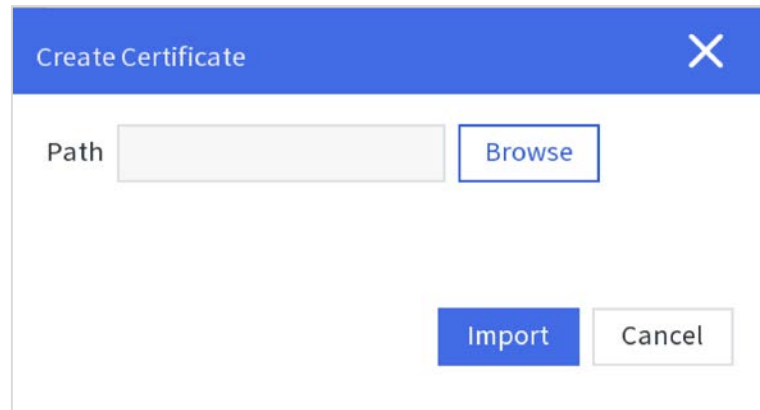
Installing Trusted CA Certificate

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.

Step 1 Select **Setting > Security > CA Certificate > Trusted CA Certificate**.

Step 2 Click **Install Trust Certificate**.

Figure 4-51 Install trusted CA certificate



- Step 3 Click **Browse** to select the certificate on the prompt interface, and then click **Import**.
After the certificate is imported successfully, you can view the created certificate on the **Device Certificate** interface.

4.1.3.6.5 A/V Encryption

The Station supports audio and video encryption during data transmission.




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

Step 1 Select **Setting > Security > A/V Encryption**.

Step 2 Configure parameters.

[illegible]

Table 4-7 Audio and video description

Encryption Type	Parameter	Description
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 as needed.

Step 3 Click **Apply**.

4.1.3.6.6 Security Warning

Security Exception

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

Step 1 Select **Setting > Security > Security Warning > Security Exception**.

Step 2 Enable security warning.




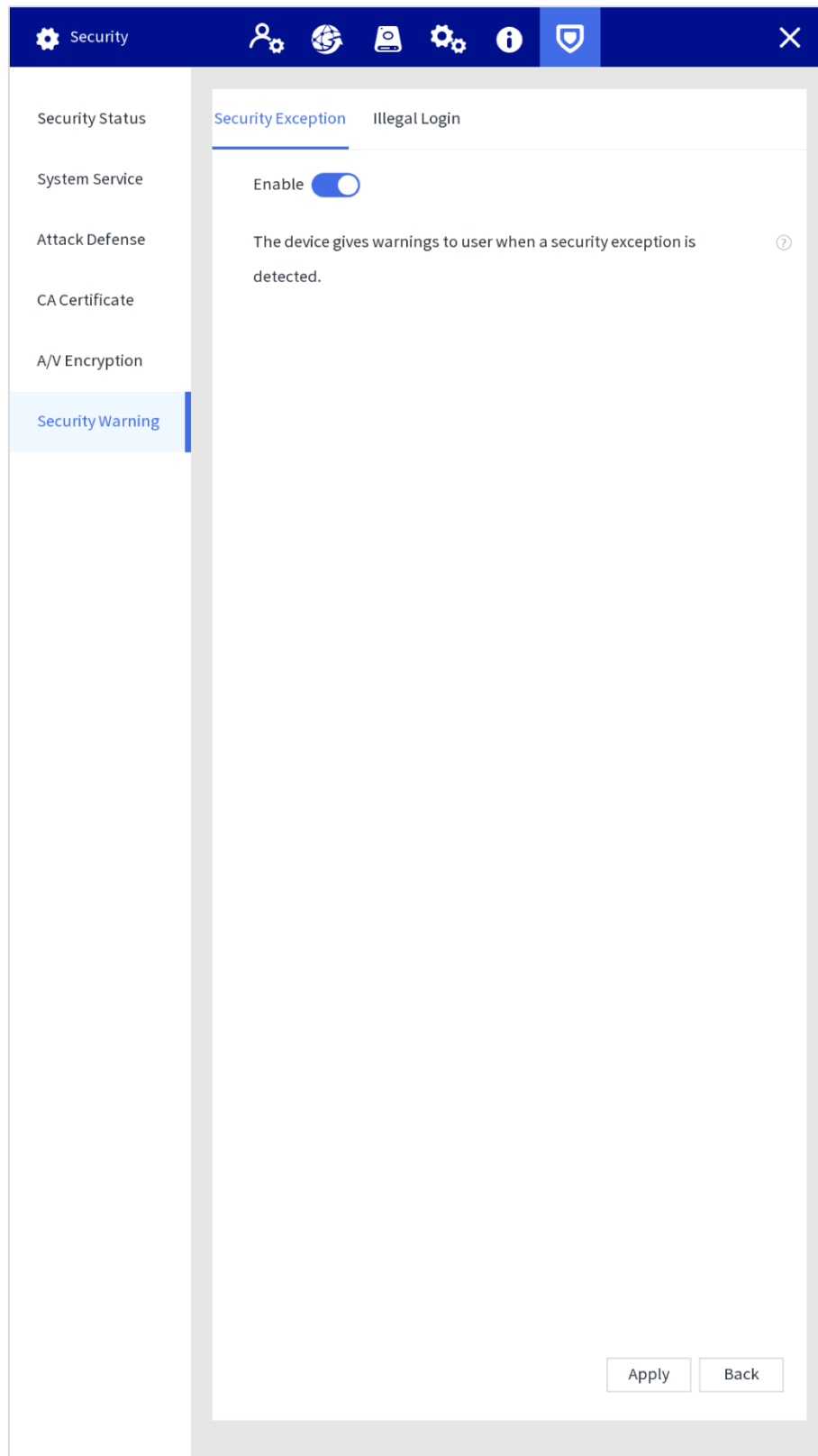
Click  to view the details of the security exception event.

Figure 4-53 Security exception



Step 3 Click **Apply**.

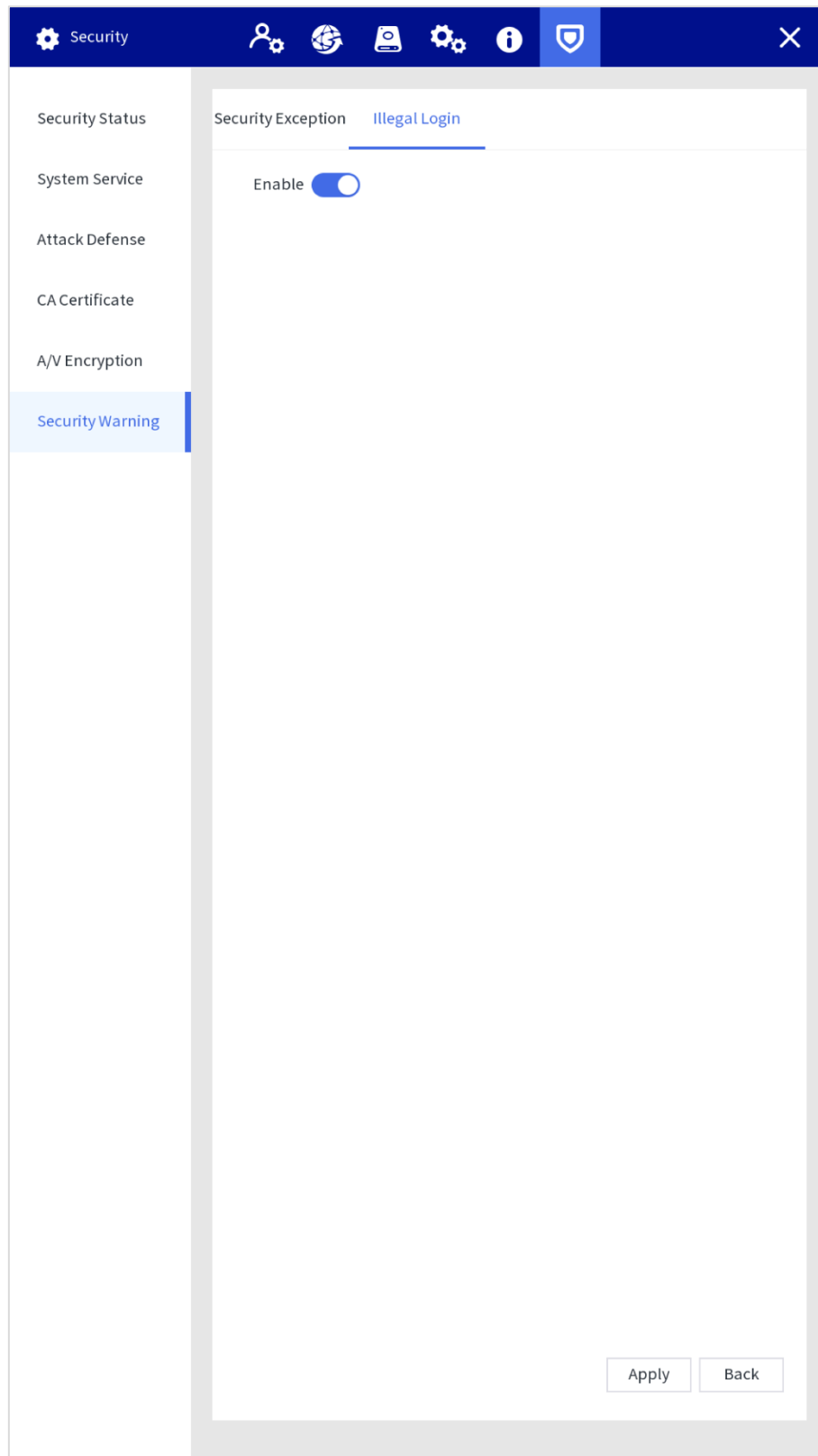
Illegal Login

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

Step 1 Select **Setting > Security > Security Warning > Illegal Login**.

Step 2 Enable illegal login warning.

Figure 4-54 Illegal login



Step 3 Click **Apply**.

4.2 Web Configuration

4.2.1 Login



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

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

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 4-55 Login

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

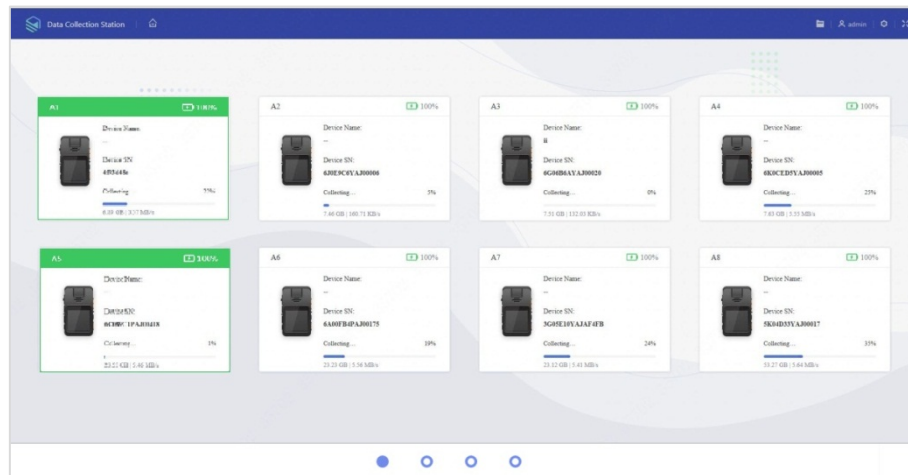
Step 3 Click **Login**.

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 4-56 Uploading files



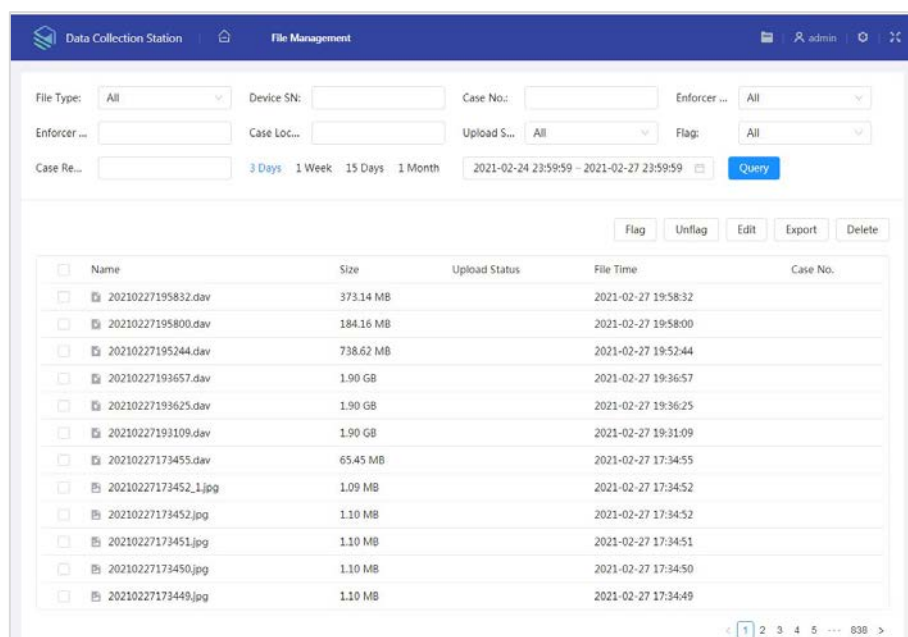
4.2.2.2 Searching for Files

Select **File Management**, and enter file type, enforcer department, upload status, device SN, enforcer No, flag, case No., case location, and case remarks, 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 4-57 Search for files



4.2.2.3 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.



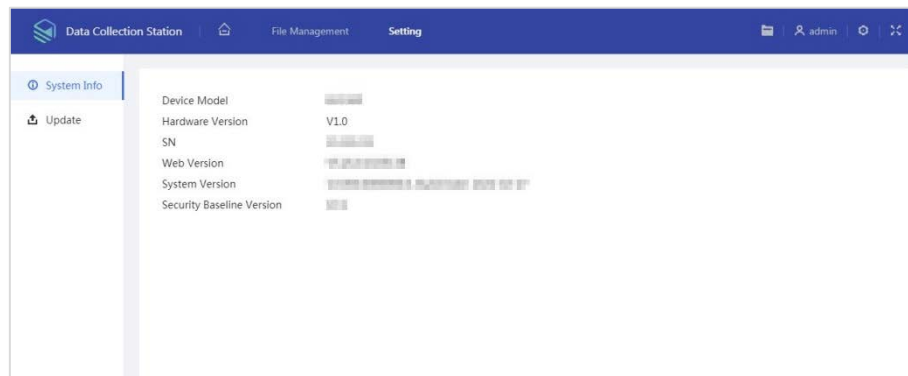
You cannot fast play or slow play an audio file in AMR format.

4.2.3 Configuring Web

4.2.3.1 System Information

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

Figure 4-58 System information



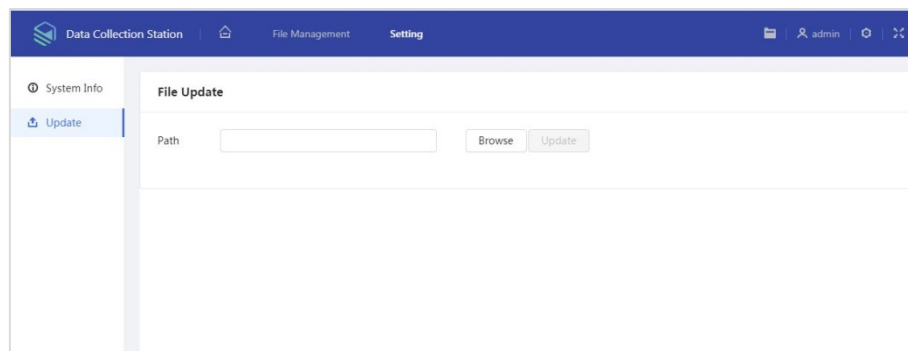
4.2.3.2 Update

Select **Setting > Update**, select the file, and then click **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.

Figure 4-59 Update



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.

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 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

Refer to the sheet for RAID space information.



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

Parameter	Total Space of the N HDD
RAID 10	$(N/2) \times \min(\text{capacityN})$
RAID 6	$(N-2) \times \min(\text{capacityN})$
RAID 5	$(N-1) \times \min(\text{capacityN})$
RAID 1	$\min(\text{capacityN})$
RAID 0	The total amount of current RAID group

Appendix 2 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.