



Dock Station

User Manual

Legal Information

©2023 Hangzhou Hikvision Digital Technology Co., Ltd. All rights reserved.

About this Manual

The Manual includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of this Manual at the Hikvision website (<https://www.hikvision.com/>).

Please use this Manual with the guidance and assistance of professionals trained in supporting the Product.

Trademarks

HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.

Other trademarks and logos mentioned are the properties of their respective owners.

Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS MANUAL AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE

Dock Station User Manual

DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 Danger	Indicates a hazardous situation which, if not avoided, will or could result in death or serious injury.
 Caution	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
 Note	Provides additional information to emphasize or supplement important points of the main text.

Contents

Chapter 1 Introduction	1
1.1 Production Introduction	1
1.2 Key Feature	1
Chapter 2 Activation and Login	2
2.1 Activation	2
2.1.1 Default Information	2
2.1.2 Activate via SADP	2
2.1.3 Activate via Web Browser	3
2.2 Login	4
Chapter 3 Basic Operation	5
3.1 Homepage	5
3.2 Access Device	5
3.3 Collect Data	6
3.4 Manage Data	6
3.4.1 Search Data	6
3.4.2 Play Back and Edit Data	6
3.4.3 Lock Data	7
3.4.4 Upload Data	8
3.4.5 Back up Data	8
3.5 Manage Storage	9
3.5.1 Manage Disk	9
3.5.2 Clean Data Automatically	9
3.5.3 Set Cloud Storage	9
3.5.4 Access Storage Server	10
3.5.5 Set Data Storage Duration	11
Chapter 4 Network	12

4.1 Set IP Address	12
4.2 Access Platform	13
4.3 Set Port	13
Chapter 5 Safety Management	14
5.1 Manage User	14
5.2 Edit Password	15
5.3 Enable HTTPS	15
5.4 Set Data Encryption	15
5.5 SSH	16
Chapter 6 Maintenance	17
6.1 View Device Information	17
6.2 Synchronize Time	17
6.3 Set DST	17
6.4 Set Local Mode	17
6.5 Search Log	18
6.6 Upgrade	18
6.6.1 Upgrade via Platform	18
6.6.2 Upgrade System	18
6.7 Reboot	19
6.8 Restore Parameters	19
6.9 Export Parameters	19
6.10 Import Parameters	20
6.11 Format Database	20
6.12 Set File Format	20
6.13 Connect to Third-Party Body Camera	21
Appendix A. Communication Matrix and Device Command	22

Chapter 1 Introduction

1.1 Production Introduction

Dock station is designed for collecting data from body cameras. It provides you a simplified way to access and back up data.

1.2 Key Feature

- Small in size, easy to place.
- Supports web operations.
- Supports collecting data from multiple body cameras.
- Supports charging, uploading data, and cleaning the storage space automatically.
- Prevents data loss via ANR (Automatic Network Replenishment).
- Adopts cyclic covering: Files will be covered automatically according to the storage timeline when there is no enough space.
- Supports reading time, date, product No., etc. of the body camera automatically.
- Supports searching files by multiple methods.
- Supports playing videos, audios, and images.
- Supports log management.

Chapter 2 Activation and Login

2.1 Activation

For the first-time access, you need to activate the device by setting an admin password. No operation is allowed before activation. The device supports multiple activation methods, such as activation via local menu, SADP software, web browser, and client software.



Refer to the user manual of client software for the activation via client software.

2.1.1 Default Information

Device default IP address and user name are as follows.

- Default IP address: 192.168.1.64
- Default user name: admin

2.1.2 Activate via SADP

SADP is a tool to detect, activate, and modify the IP address of the devices over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website <http://www.hikvision.com/>, and install it according to the prompts.
- The device and the computer that runs the SADP tool should belong to the same network segment.

The following steps show how to activate one device and modify its IP address. For batch activation and IP address modification, refer to *User Manual of SADP* for details.

Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Enter a new password (admin password) and confirm the password.



STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Click **Activate** to start activation.

Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

4. Click **OK** to complete activation.
5. Go to the network settings interface to modify IP address of the device.

2.2 Login

You can log in to the device via web browser for further operations such as live view and local configuration.

Before You Start

Connect the device to the network directly, or via a switch or a router.

Steps

1. Open the web browser, and enter the IP address of the device to enter the login interface.
2. Enter **User Name** and **Password**.
3. Click **Login**.
4. Download and install appropriate plug-in for your web browser. Follow the installation prompts to install the plug-in.
5. Reopen the web browser after the installation of the plug-in and repeat steps 1 to 3 to login.
6. **Optional:** Click **Logout** on the upper right corner of the interface to log out of the device.

Chapter 3 Basic Operation

3.1 Homepage

Check the collection and storage status of body cameras in the homepage.

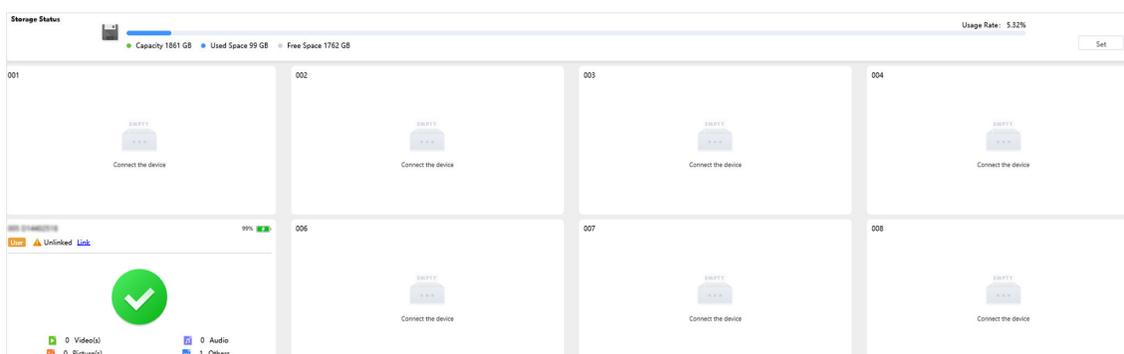


Figure 3-1 Homepage

3.2 Access Device

Add a body camera and start collecting.

Before You Start

- Connect a body camera to the dock station.
- Go to **System** → **System Maintenance** → **Local Mode** to enable **Local Mode**.
- Add a user according to "User Management" if you need to link to a user.

Steps

1. Click **Device Management**.
2. Click **Add Device**.
3. Enter **Device Name** and **Device No.**

Note

The device No. should be the same with that of the body camera.

4. **Optional:** Select a person.
5. Click **OK**.
6. **Optional:** You can also do the following operations.

- | | |
|--------------------------------|---|
| Search Device | Enter conditions and click Search . |
| Edit Device Information | Click  to edit device information. |
| Delete Device | Select a device and click  . |

Import/Export Device Information

If you want to reuse the device information, you can click **Export** to export device information to the local storage and import it to a new device.

3.3 Collect Data

The dock station starts to collect data after a body camera is connected.

If the body camera is unassociated to the person, you can click **Link** to associate.

During the data collection, enable **Prior Collection** and the file collection of other body camera(s) will stop until the priority collection finishes. During the prior collection process, you can disable **Prior Collection**.

3.4 Manage Data

3.4.1 Search Data

You can search collected data.

Steps

1. Click **File Management**.
2. Enter or select conditions.
3. Click **Search**.

Result

The searched data will be displayed.

3.4.2 Play Back and Edit Data

You can play back and edit data.

Steps

1. Click **File Management**.
2. Enter conditions and click **Search**.
3. Click the file thumbnail to play.

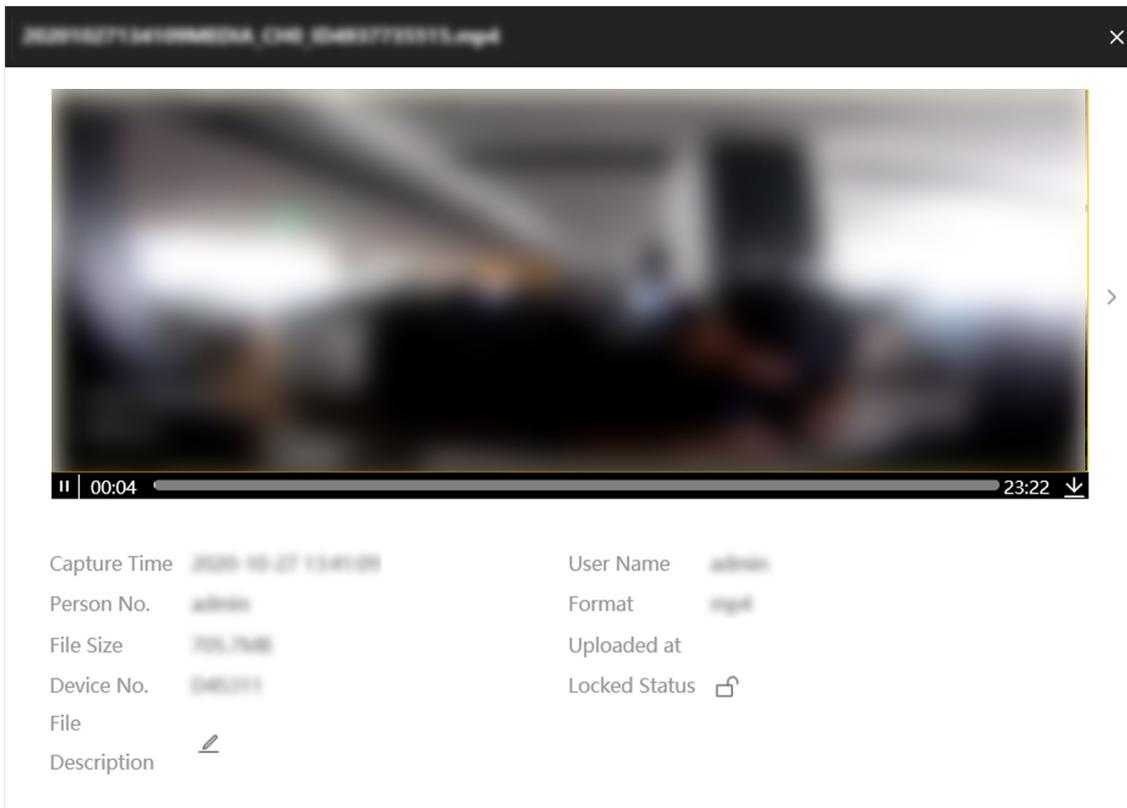


Figure 3-2 Playback

Note

- If it is a picture file, when you place the cursor on the left side, the area will be magnified on the right side.
- Playback interfaces may vary with file types.

4. Optional: Click [↗](#) to add descriptions to the played file and click **OK**.

5. Optional: You can also do the following operations.

-  Start playing.
-  Stop playing.
-  Download the file to the local storage on the playback page.
-  View the previous/next file.

3.4.3 Lock Data

Lock important data to prevent them from being overwritten or accidentally deleted.

Steps

- 1. Click File Management.**

2. Enter conditions and click **Search**.

3. You can lock or unlock data.

- Click  in the row to lock a single record. Click  to unlock.
- Check several records and click **Lock** to lock them in batch. Click **Unlock** to unlock.

Result

The locked data cannot be deleted or overwritten.

3.4.4 Upload Data

The device can upload data to the platform after connected to it.

Before You Start

The device has been connected to the platform.

Steps

1. Click **File Management**.

2. Enter conditions and click **Search**.

3. Check files that need to be uploaded.

- Click  in the row to upload a single record.
- Check several records and click **Upload** to upload them in batch.
- Click **Upload All** to upload all the records.

4. Click **Upload**.



Note

If you enable the backup and set a storage server type in **Storage Settings → Storage Management**, data will be synchronized to the set server.

3.4.5 Back up Data

You can back up data by downloading it to the local storage.

Steps

1. Click **File Management**.

2. Enter conditions and click **Search**.

3. Download data.

Download a single record

- a. Click  in the row to lock a single record.
- b. Select **Download to Computer**, **Download to USB Flash Drive** or **Download to FTP**.
- c. Click **OK**.

- Download records in batch**
- a. Check several records and click **Download**.
 - b. Select **Download to Computer**, **Download to USB Flash Drive** or **Download to FTP**.
 - c. Click **OK**.

3.5 Manage Storage

3.5.1 Manage Disk

You can view the disk capacity and status, or format the disk.

Steps

1. Go to **Storage Settings → Disk** .
2. View the disk capacity, free space, status, etc.
3. **Optional:** Format the disk.
 - 1) Check the disk(s) to be formatted.
 - 2) Click **Format**.
 - 3) Click **OK**.

3.5.2 Clean Data Automatically

The device can delete data automatically when there is no enough space.

Steps

1. Go to **Storage Settings → Storage Management → Storage Parameters Settings** .
2. Enable **Clear Body Camera Data**.
3. Set **Disk Min. Free Space** and **Cleaned Space Once**.



Caution

Back up or lock important data in time in case of data loss. The device will delete the earliest data when there is no enough space.

Example

If you set **Disk Min. Free Space** to **10** and **Cleaned Space Once** to **5**, the device will clean 5 G automatically when the space is less than 10 G.

4. Click **Save**.

3.5.3 Set Cloud Storage

Cloud storage is a kind of network storage. It can be used as the extended storage to save the collected data.

Before You Start

- Arrange the cloud storage server.
- The communication between the device and server is normal.

Steps

1. Go to **Storage Settings** → **Storage Management** → **Storage Server Settings** .

Storage Server Settings

Enable Backup

Storage Server Type

* IP Address

* Port

* Bucket

* AKEY

* SKEY

poolID

Save

Figure 3-3 Set Cloud Storage

2. Enable backup.
3. Set **Storage Server Type** as **CSTOR**.
4. Set other parameters according to the actual needs.
5. Click **Save**.

3.5.4 Access Storage Server

Storage server can be used as an extended storage to store data of body cameras.

Before You Start

- Arrange the cloud storage server.
- The communication between the device and server is normal.

Steps

1. Go to **Storage Settings** → **Storage Management** → **Storage Server Settings** .

2. Enable backup.
3. Set **Storage Server Type** as **CVR**.
4. Enter **IP Address, Port**, etc.
5. Click **Save**.

3.5.5 Set Data Storage Duration

You can set the data storage duration of the device.

Steps

1. Go to **Storage Settings → Storage Management → Storage Duration Settings** .
2. Enable the storage duration.
3. Select **Storage Duration Type**.
4. Click **Save**.

What to do next

Data that exceeds the storage duration will be deleted automatically.

Chapter 4 Network

4.1 Set IP Address

You can set an IP address if you need to operate the device over network.

Steps

1. Go to **Network Settings** → **TCP/IP** .

The screenshot shows a network configuration window with the following fields and values:

- NIC Type: 10M/100M/1000M Self-adap (dropdown menu)
- Automatic Gain: (disabled)
- * IPv4 Address: 10.10.98.241
- * IPv4 Subnet Mask: 255.255.255.0
- * IPv4 Default Gateway: 10.10.98.254
- MAC Address: 00:40:3a:45:27:9c
- MTU: 1500 (with minus and plus buttons)
- * Preferred DNS Server: 0.0.0.0
- * Alternative DNS Server: 0.0.0.0

A red "Save" button is located at the bottom center of the form.

Figure 4-1 Set IP Address

2. Select **NIC Type**.
3. Set other parameters according to the actual needs.

Note

- Enable **Automatic Gain** to get the IP address, subnet mask, and default gateway automatically if the network supports distributing the IP address automatically.
- MTU: It stands for maximum transmission unit. It is the size of the largest protocol data unit that can be communicated in a single network layer transaction.
- Preferred DNS Server and Alternative DNS Server are reserved.

4. Click **Save**.
-

4.2 Access Platform

Access the platform to upload data or receive information.

Before You Start

- Arrange the cloud storage server.
- The communication between the device and server is normal.

Steps

1. Go to **Network Settings** → **Platform Settings** .
2. Enter **IP Address**, **Port**, **Person Name**, and **Password**.
3. **Optional**: Enable the uploading plan and set **Start Time** and **End Time** to upload data in a fixed time period.



Note

If this function is disabled, data will be uploaded to the platform in real time.

4. Click **Save**.

Result

View the platform connection status on the top right corner of the interface. You can upload data if the platform is connected. Check the platform information and communication if connection failed.

4.3 Set Port

The device port can be modified when the device cannot access the network due to port conflicts.

Steps

1. Go to **System** → **System Settings** → **Port** .
2. View or edit the port.

HTTP Port

It refers to the port through which the browser accesses the device. For example, when the **HTTP Port** is modified to 81, you need to enter ***http://192.168.1.64:81*** in the browser for login.

HTTPS Port

It refers to the port through which the browser accesses the device, but certificate verification is needed.

3. Click **Save**.

Chapter 5 Safety Management

5.1 Manage User

In order to enhance data security, it is recommended to differentiate users to manage data and avoid multiple users to manage devices by the same account.

Before You Start

Go to **System** → **System Maintenance** → **Local Mode** to enable **Local Mode**.

Steps

1. Click **Person Management**.
2. Add a user.



Note

Go to **System** → **System Maintenance** → **Local Mode** to enable **Local Mode**, then you can add a user.

- 1) Click **Add User**.
- 2) Enter the user information, such as **User No.**, **Password**, etc.
- 3) Set the user's permissions.

File Search Permission

This permission is enabled by default. If you disable the permission, the person cannot manage the files collected from the associated body camera.

Super Admin Permission

If you enable this permission, the person can view and manage all the files collected from all the connected body cameras, no matter which body camera is associated with him or her. If you disable this permission, the person can only view and manage the files collected from the body cameras associated with him or her.

- 4) Click **OK**.
- 5) Link the user to the device in the device management interface.

You can search the linked data after logging in with the added person No. and password.

3. Enter conditions and click **Search** to get user information.
4. **Optional:** When you need to set the same user information to another dock station, you can export or import the user information.

Export Click **Export**, and select a path to save the file.

- Import**
- a. Click **Import**.
 - b. Download the import template, edit it, and save it in the computer.
 - c. Click **Select File**, and select the user information template saving in the computer.
 - d. Click **Import**.

5. **Optional:** You can do the following operations.

Edit user information	Click  to edit the user information.
Delete user information	<ul style="list-style-type: none">• Click  to delete the user information.• Check several user information and click Delete to delete them in batch.

5.2 Edit Password

You are recommended to change the device password regularly to enhance data security.

Steps

1. Go to **admin** → **Change Password** .
2. Enter **Old Password**.
3. Enter **New Password** and confirm it.
4. Click **OK**.

Result

Next time you log in to the device, use the new password.

5.3 Enable HTTPS

If the demand for external access security is high, you can enable HTTPS protocol to ensure the data transmission security.

Steps

1. Go to **System** → **System Settings** → **HTTPS** .
2. Check **Enable HTTPS**.

5.4 Set Data Encryption

Set data encryption to encrypt the uploaded data from the body cameras to enhance security.

Steps

1. Go to **System** → **System Settings** → **Encryption** .
2. Enable **Status**.
3. Select **Encryption Type**.
4. Enter **Encryption Key**.
5. Click **Save**.

Result

Use the dedicated player and enter the key to play the encrypted videos.

5.5 SSH

To raise network security, disable SSH service. The configuration is only used to debug the device for the professionals.

Steps

1. Go to **System** → **System Maintenance** → **Enable SSH service** .
2. Set the SSH service.
3. Click **OK**.

Chapter 6 Maintenance

6.1 View Device Information

Go to **System** → **System Settings** → **Device Information** to edit the device name or view the device information such as dock station No., serial No., system version, etc.

6.2 Synchronize Time

Synchronize the device time when it is inconsistent with the actual time.

Steps

1. Go to **System** → **System Settings** → **Set Time** .
2. Select **Time Zone**.
 - Select **Set Time** to synchronize time manually.
 - Enable **Synchronize with computer time** to synchronize the device time with that of the computer automatically.
3. Set the device time.
 - Select **Manual Time Sync** to synchronize the device time with that of the computer. Set time manually, or enable **Sync. with computer time**.
 - Select **NTP Time Sync** to synchronize the device time with that of the NTP sever. Set **Server Address**, **NTP Port**, and **Time Sync Interval**. Click **NTP Test** to test if the connection between the device and the server is normal.
4. Click **Save**.

6.3 Set DST

If the region where the device is located adopts Daylight Saving Time (DST), you can set this function.

Steps

1. Go to **System** → **System Settings** → **DST** .
2. Enable DST.
3. Set **Start Time**, **End Time**, and **Time Bias**.
4. Click **Save**.

6.4 Set Local Mode

You can enable local mode to add devices and users.

Steps

1. Go to **System** → **System Maintenance** → **Local Mode** .
2. Enable **Local Mode**.

6.5 Search Log

You can view historical records by searching logs.

Steps

1. Go to **System** → **Log Search** .
2. Set conditions.
3. Click **Search**.
Logs will be displayed.
4. **Optional**: Click **Export** to save logs to your computer.

6.6 Upgrade

6.6.1 Upgrade via Platform

You can upgrade the device program sent by the platform.

Before You Start

Connect the device to the platform.

Steps

1. Go to **System** → **System Settings** → **Upgrade** .
2. Select **Station Host**.
3. Select **Work Mode** as **Acquisition Mode**.
4. Click **Upgrade**.
5. Enter the password and click **OK**.
6. **Optional**: Select **Work Mode** as **Upgrade Mode** to upgrade the body camera(s).

6.6.2 Upgrade System

Upgrade the system when you need to update the device version.

Before You Start

Save the upgrade file to the computer.

Steps

1. Go to **System** → **System Maintenance** → **Device Upgrade** .
2. Click **Select File** and select an upgrade file.

3. Click **Upgrade**.

Note

- The dock station will stop collecting during upgrade.
 - Do not cut off the power supply. The body cameras will reboot automatically after upgrade.
-

6.7 Reboot

When the device needs to be rebooted, reboot it via the web page instead of cutting off the power directly.

Steps

1. Go to **System** → **System Maintenance** → **Reboot** .
2. Click **Reboot**.
3. Click **OK**.

6.8 Restore Parameters

When the device is abnormal caused by the incorrect set parameters, you can restore the parameters.

Steps

1. Go to **System** → **System Maintenance** → **Restore Default Settings** .
2. Select the restoration mode.
 - Click **Restore Default Settings** to restore the parameters except the IP parameters and user parameters to the default settings.
 - Click **Restore all parameters** to restore all the parameters to the factory settings.
3. Click **OK**.

6.9 Export Parameters

You can export the parameters of one device, and import them to another device to set the two devices with the same parameters.

Steps

1. Go to **System** → **System Maintenance** → **Exporting configuration parameters** .
2. Click **Export**.
3. Click **OK** and export the parameters according to the prompts.

6.10 Import Parameters

Import the configuration file of another device to the current device to set the same parameters.

Before You Start

Save the file that needs to be imported to the computer.

Steps



Note

Importing configuration file is only available to the devices of the same model and same version.

1. Go to **System** → **System Maintenance** → **Importing configuration parameters** .
2. Click **Select File** to import the configuration file.
3. Click **Import**.

Result

The parameters will be imported, and the device will reboot.

6.11 Format Database

If you want to clear all the local data of the dock station, you can format database.

Steps



Caution

The database will be cleared after formatting. Operate the function carefully.

1. Go to **System** → **System Maintenance** → **Formatting HDD** .
2. Click **Format**.
3. Enter the password on the popup window.
4. Click **OK**.

6.12 Set File Format

The device supports setting file formats that can be collected.

Steps

1. Go to **Storage Settings** → **File Format Settings** .
2. Check file formats according to the actual needs.
3. **Optional:** Add new formats and use / to separate them.
4. Click **Save**.

6.13 Connect to Third-Party Body Camera

The device can connect body cameras from the third-party manufacturers to collect files.

Steps

1. Go to **System** → **System Settings** → **Manufacturer** .
2. Select the manufacturer.
3. Click **Save**.

Result

The device will connect the third-party body cameras according to the selected manufacturer protocols and collect files.

Appendix A. Communication Matrix and Device Command

Scan the QR code below to get the communication matrix of the device.



Scan the QR code below to get the device command.





See Far, Go Further