Desktop Dock Station

User Manual

Legal Information

About this Document

- This Document 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 Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- 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.
- HDMI The terms HDMI and HDMI High-Definition Multimedia Interface, and the HDMI Logo are trademarks or registered trademarks of HDMI Licensing Administrator, Inc. in the United States and other countries.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT 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 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 DOCUMENT 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 Product 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 SADP software and web browser.

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.

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 **Activate** to start activation.

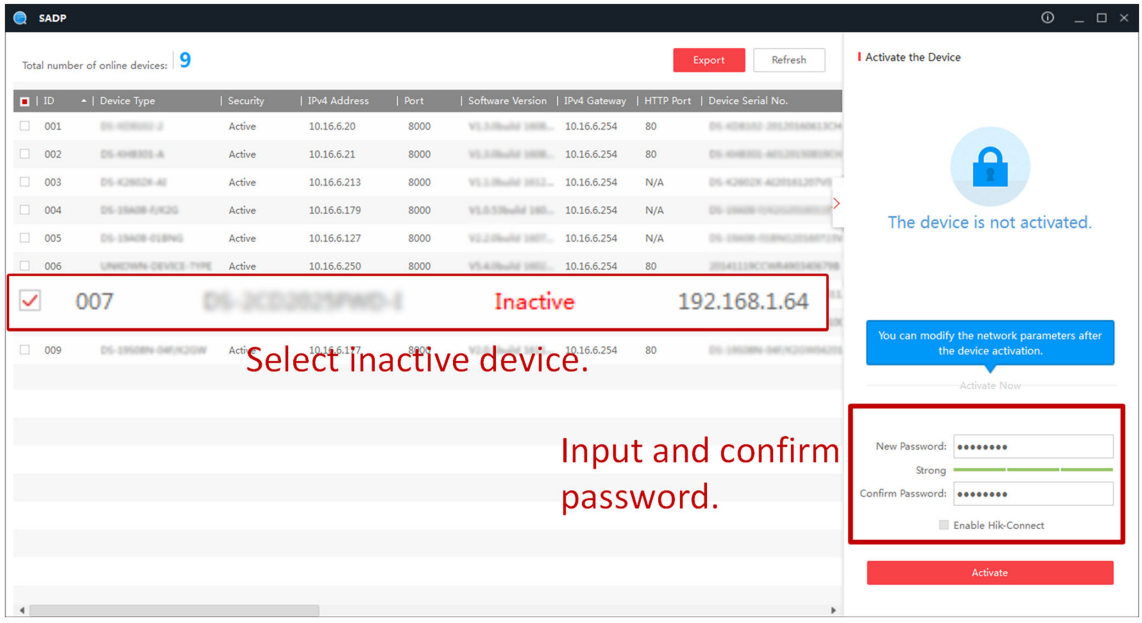


Figure 2-1 Activate via SADP

Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.
   1) Select the device.
   2) Change the device IP address to the same network segment as your computer by either modifying the IP address manually or checking **Enable DHCP**.
   3) Enter the admin password and click **Modify** to activate your IP address modification.

2.1.3 Activate via Web Browser

Use web browser to activate the device. For the device with the DHCP enabled by default, use SADP software or client software to activate the device.

Before You Start

Ensure the device and the computer connect to the same LAN.

Steps

1. Change the IP address of your computer to the same network segment as the device.
2. Open the web browser, and enter the default IP address of the device to enter the activation interface.
3. Create and confirm the admin password.

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 Homepage

The dock station starts to collect files after a body camera is connected. Click **Homepage** to view the storage status of the dock station and the file collection status of the connected body cameras.

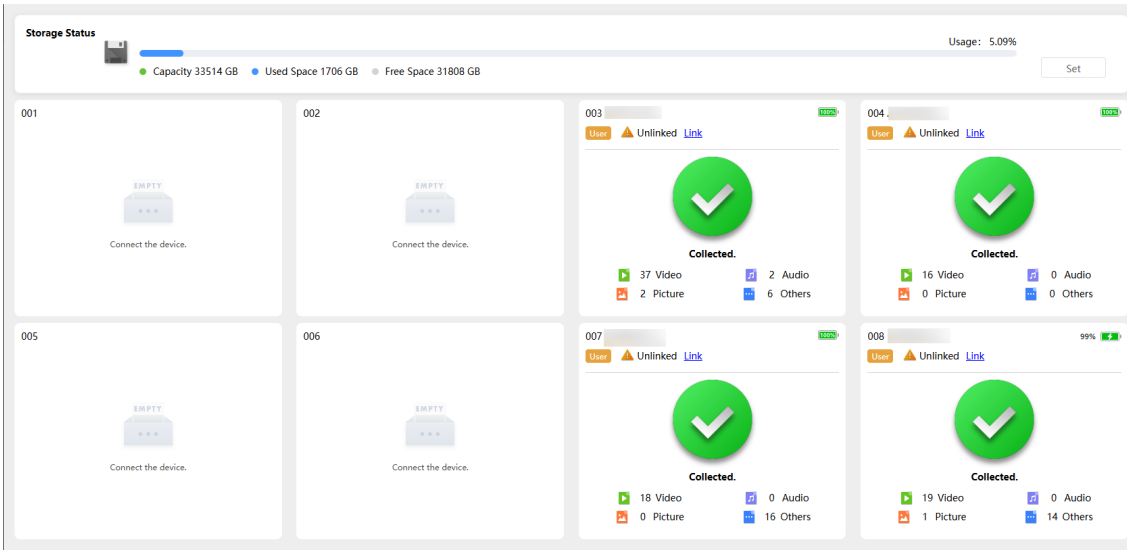


Figure 3-1 Homepage

- If the body camera is not linked to a person, you can click **Link** to link a person. Add a person first. Refer to ***Person Management*** for details.
- During the collection process, enable **Prior Collection** and the file collection of other body camera(s) will stop until the prior collection finishes. During the prior collection process, you can disable **Prior Collection**.

Chapter 4 Device Management

After you connect a body camera to the dock station, the dock station will add the body camera and get the body camera No. automatically. You can also add body cameras manually.

Before You Start

- Connect a body camera to the dock station.
- Go to **System → System Maintenance → Local Mode** to enable **Local Mode**.
- Add persons according to ***Person Management*** if you want to link persons to the body cameras.

Steps

1. Click **Device Management**.

   The connected body camera No. and linked person information will be displayed.

Figure 4-1 Device Management

2. Add a body camera.

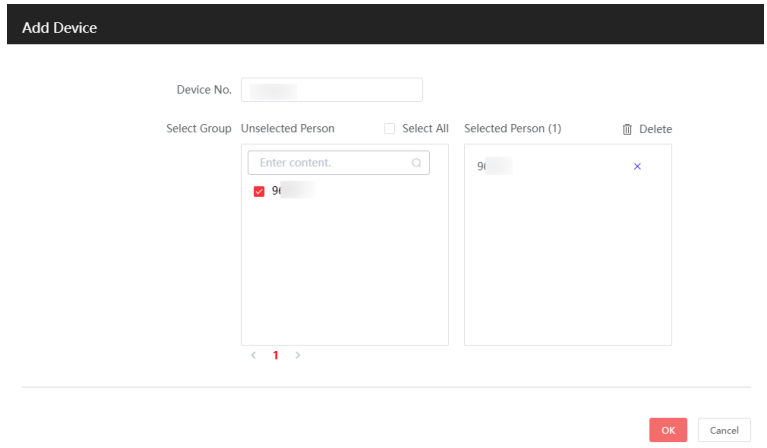


Figure 4-2 Add Device

1) Click **Add**.
2) Enter **Device No.**

Note

The device No. is the serial No. of the body camera. You can get the No. from the body camera label or enter the body camera local menu to view the No.

3) **Optional:** If you want to link a person to the body camera, select a person.
4) Click **OK**.

3. **Optional:** You can also do the following operations.

Search device	Enter **Device No.** and click **Search** to search the added device. You can click **Reset** to reset the search conditions.
Change the device linked person	Click to change the device linked person.
Delete device	• Click after the added device item to delete the device. • Select the added device(s), and click **Delete** on the upper menu to delete the selected device(s).
Import devices	You can import device(s) in batch. a. Click **Import**. b. Click **template.xlsx** to download the template to the computer. c. Fill in the template and save it to the computer. d. Return to **Device Management** interface, and click **Import → Select File** to select the edited template. Click **Import** to import the device(s) in batch.
Export device information	Click **Export** to export the added device information to the computer for importing it to other dock stations.

Chapter 5 Person Management

You can add, edit, or delete persons to link to the connected body cameras.

Before You Start
Go to **System → System Maintenance → Local Mode** to enable **Local Mode**.

Steps
1. Click **Person Management**.
2. Add a person.

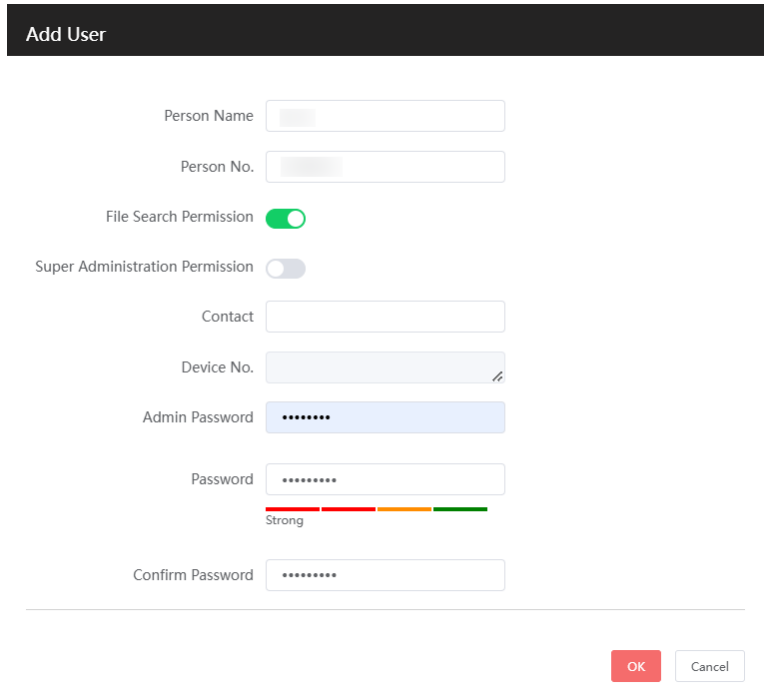


Figure 5-1 Add Person

1) Click **Add**.
2) Enter the person information, such as **Person Name**, **Person No.**, etc.
3) Set the person'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 linked body camera.

Super Administrator 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 linked with him or her. If you disable this permission, the person can only view and manage the files collected from the body cameras linked with him or her.

4) Enter **Admin Password**.
5) Set **Password** for the person, and confirm the password.

Note

The set password is used for taking the linked body camera out. It will also be applied to the linked body camera, and you need to enter the password to log in to the body camera.

6) Click **OK**.

3. **Optional:** You can also do the following operations.

Search person	Enter **Person Name** or **Person No.**, and click **Search** to search the added person. You can click **Reset** to reset the search conditions.
Edit person information	Click ✎ to edit the person information.
Delete person	• Click 🗑 after the added person item to delete the person. • Select the added person(s), and click **Delete** on the upper menu to delete the selected person(s).
Import persons	You can import person(s) in batch. a. Click **Import**. b. Click **template.xlsx** to download the template to the computer. c. Fill in the template and save it to the computer. d. Return to **Person Management** interface, and click **Import → Select File** to select the edited template. Click **Import** to import the person(s) in batch. **Note** The device No. will not be imported.
Export person information	Click **Export** and enter **Admin Password** to export the added person information to the computer for importing it to other dock stations.

Chapter 6 File Management

The dock station starts to collect files after a body camera is connected. You can view the file information, play back files, download files, etc.

Before You Start

Connect the body cameras to the dock station.

Steps

1. Click **File Management**.

   The collected files will be displayed in the list.

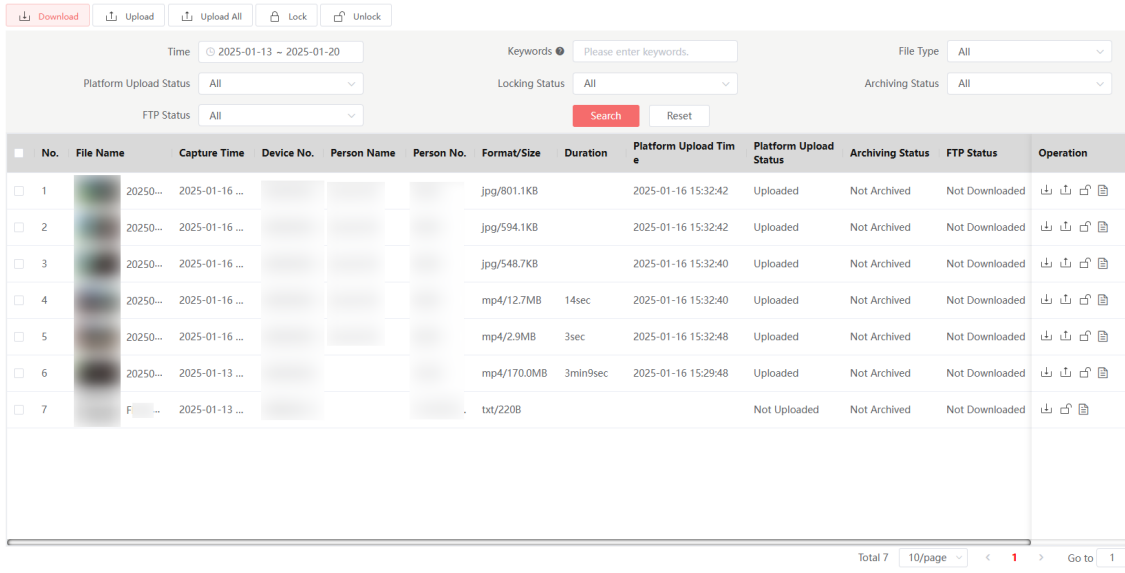


Figure 6-1 File Management

2. You can click the file thumbnail to play back the file and view the file details.

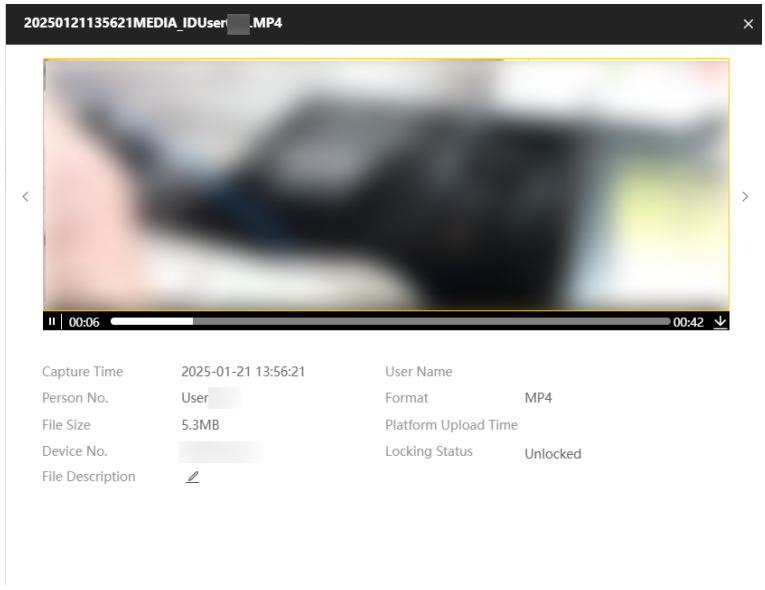


Figure 6-2 Play back File

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.
- You can click ✎ to add descriptions to the played file and click **OK**.
- If it is a video file, you can click ▶ / ⏸ to start/stop playback.
- You can click ⬇ to download the file to the computer.
- You can click ‹ / › to view the previous/next file.

3. **Optional:** You can also do the following operations.

Search files	Set the search conditions and click **Search** to search the files. You can click **Reset** to reset the search conditions.
Download files	• Click ⬇ after a file item to download the single file. Select the path to save the file, including the computer, USB flash drive (if a USB flash drive is connected to the dock station), and FTP. • Select the file(s) to be downloaded, and click **Download** on the upper menu. Select the path to save the file, including the computer, USB flash drive (if a USB flash drive is connected to the dock station), and FTP.
Upload files to the connected platform	• Click ⬆ after a file item to upload it to the connected platform. • Select the file(s) to be uploaded, and click **Upload** on the upper menu to upload the selected file(s) to the connected platform. • Click **Upload All** on the upper menu to upload all the files to the connected platform.
Lock files	You can lock important files to prevent them from being overwritten or accidentally deleted.

	• Click after a file item to lock it. • Select the file(s) to be locked, and click **Lock** on the upper menu to lock the selected file(s).
Unlock files	• Click after a locked file item to unlock it. • Select the file(s) to be unlocked, and click **Unlock** on the upper menu to unlock the selected file(s).
Play back file and view file details	Click to play back the file and view the file details.

Chapter 7 Storage Settings

7.1 Format Disk

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

Steps

1. Go to **Storage Settings → Disk** .

Figure 7-1 Disk

2. View the disk capacity, free space, status, etc.
3. **Optional:** Format the disk.

Caution

Formatting will clear all the data stored in the disk. Back up data before formatting.

1) Select the disk(s) to be formatted.
2) Click **Format**.
3) Enter the admin password, and click **OK**.

7.2 Manage Disk Capacity

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**.

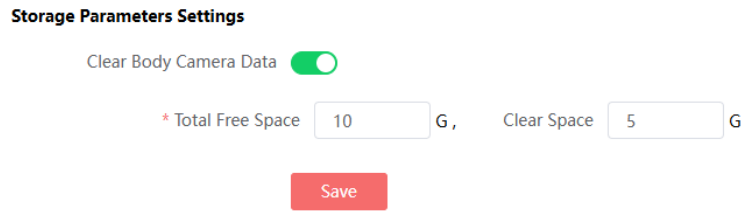


Figure 7-2 Clear Body Camera Data

3. Set **Total Free Space** and **Clear Space**.

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 **Total Free Space** to ***10*** and **Clear Space** to ***5***, the device will clean 5 G automatically when the free space is less than 10 G.

4. Click **Save**.

7.3 Set CVR Storage

CVR (Central Video Recorder) is a dedicated storage technology integrating device management, video management, and transmission. The dock station supports uploading collected files to the CVR storage server.

Before You Start

- Arrange the CVR storage server.
- The communication between the dock station and the server is normal.

Steps

1. Go to **Storage Settings → Storage Management → Storage Server Settings** .
2. Enable backup.
3. Select **Storage Server Type** as **CVR**.

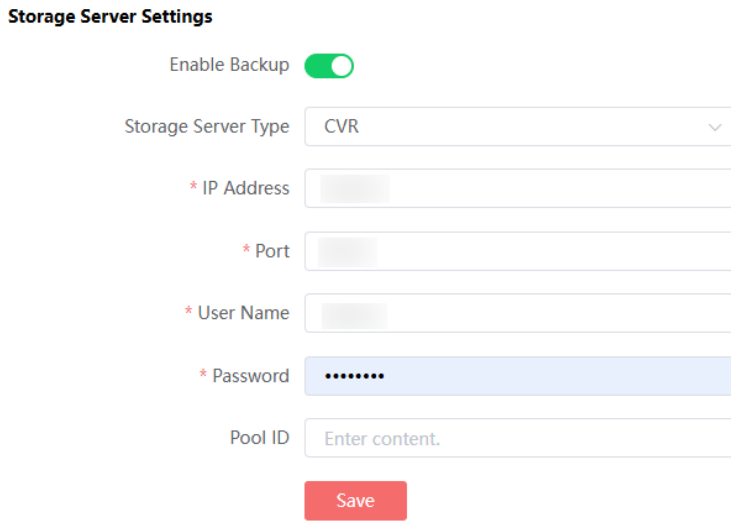


Figure 7-3 Set CVR Storage

4. Enter **IP Address** and **Port** of the server, and **User Name** and **Password** when logging in to the server.
5. Click **Save**.

7.4 Set CSTOR Storage

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

Before You Start

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

Steps

1. Go to **Storage Settings → Storage Management → Storage Server Settings** .
2. Enable backup.
3. Select **Storage Server Type** as **CSTOR**.

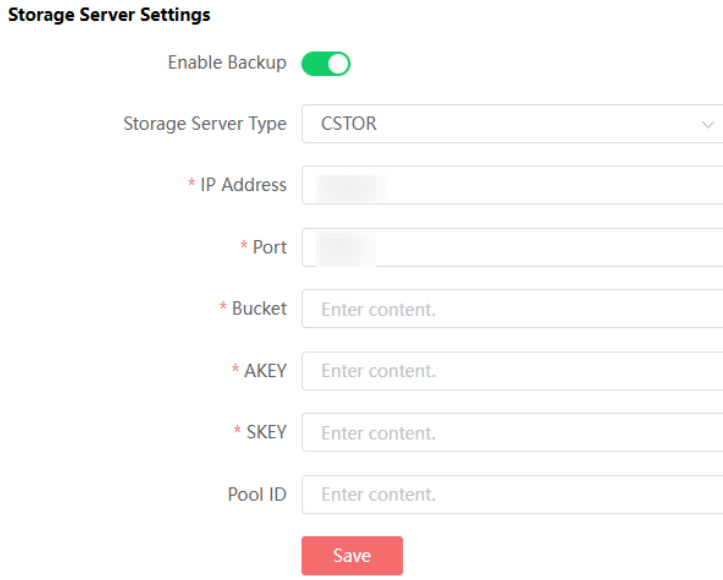


Figure 7-4 Set CSTOR Storage

4. Set the parameters of the storage server.
5. Click **Save**.

7.5 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.

7.6 Set File Format

You can set file formats to be collected by the dock station.

Steps

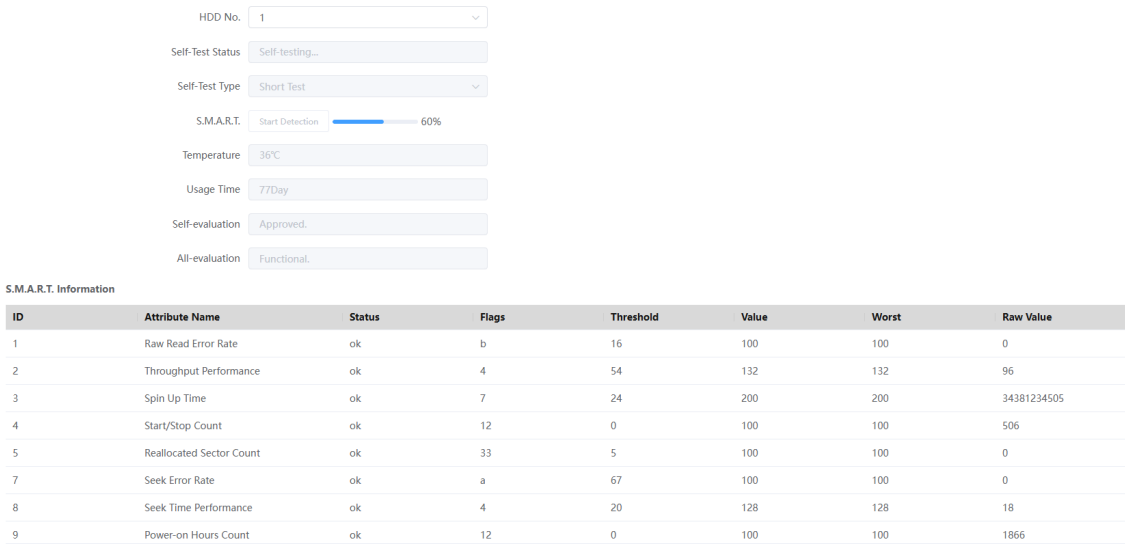
1. Go to **Storage Settings → File Format Settings** .
2. Select file formats according to the actual needs.
3. **Optional:** If you want to add more formats, click **Add Format**. Click **Add** and enter the format. Click **OK**.
4. **Optional:** If you want to add other formats except the video, audio, and picture formats, enter **Custom Format** and use / to separate them.
5. Click **Save**.

7.7 S.M.A.R.T. Detection

S.M.A.R.T. (Self-Monitoring, Analysis and Reporting Technology) is a monitoring system for HDD to detect and report on various indicators of reliability in the hopes of anticipating failures.

Steps

1. Go to **Storage Settings → S.M.A.R.T. Detection** .



ID	Attribute Name	Status	Flags	Threshold	Value	Worst	Raw Value
1	Raw Read Error Rate	ok	b	16	100	100	0
2	Throughput Performance	ok	4	54	132	132	96
3	Spin Up Time	ok	7	24	200	200	34381234505
4	Start/Stop Count	ok	12	0	100	100	506
5	Reallocated Sector Count	ok	33	5	100	100	0
7	Seek Error Rate	ok	a	67	100	100	0
8	Seek Time Performance	ok	4	20	128	128	18
9	Power-on Hours Count	ok	12	0	100	100	1866

Figure 7-5 S.M.A.R.T. Detection

2. Select **HDD No.**
3. Select **Self-Test Type**.

Short Test

A rapid mode to test the HDD key part to evaluate its health status.

Expanded Test

A comprehensive and further test to test all the parts of the HDD, including the redundant areas and areas which may exist potential problems. It will consume more time.

Conveyance Test

A test to detect the HDD R/W speed and data transmission stability.

4. Click **Start Detection**, and view the detection result in the list.

7.8 Bad Sector Test

You can detect the bad sector of HDD to check the status.

Steps

1. Go to **Storage Settings → Bad Sector Test** .
2. Select **HDD No.**
3. Select **Detection Mode** as **Full Detection** or **Key Area Detection**.
4. Click **Start Detection**, and view the detection result below.

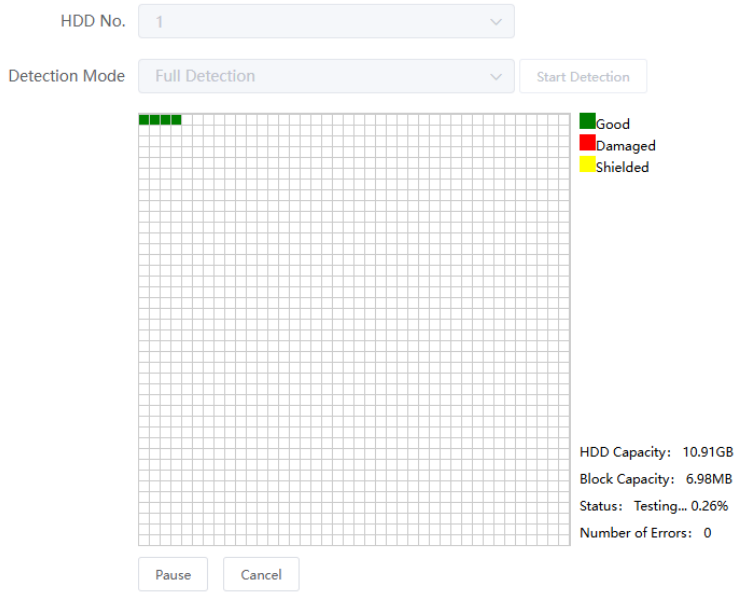


Figure 7-6 Bad Sector Test

Note

You can pause/restore or cancel the detection.

Chapter 8 Network Settings

8.1 Set IP Address

IP address must be properly configured before you operate the device over network.

Steps

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

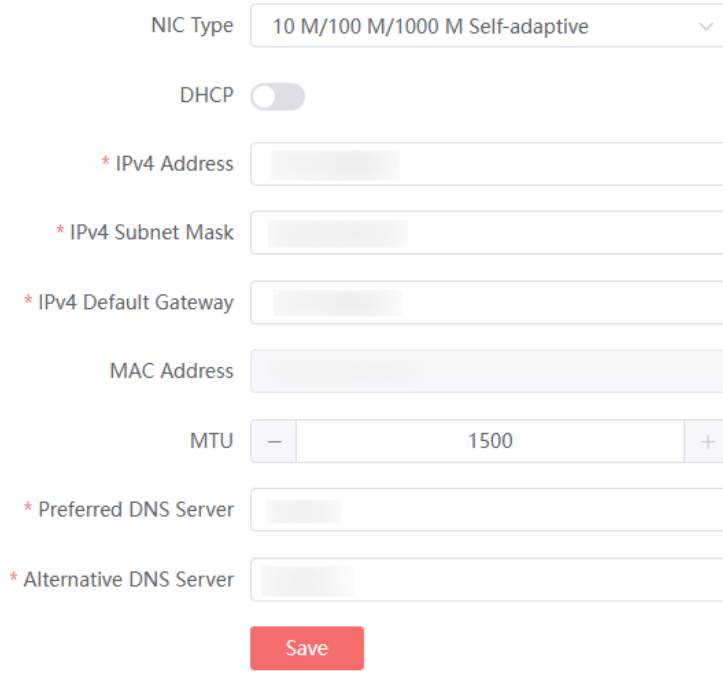


Figure 8-1 Set IP Address

2. Select **NIC Type**.
3. Set network parameters in two ways.
   - Enable **DHCP** to get the IP address, subnet mask, and default gateway automatically if the network supports distributing the IP address automatically.
   - Disable **DHCP**, and set **IPv4 Address**, **IPv4 Subnet Mask**, and **IPv4 Default Gateway** manually.
4. Set other parameters.

   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.

   DNS

It stands for domain name server. It is required if you need to visit the device with domain name. And it is also required for some applications (e.g., sending email). Set **Preferred DNS Address** and **Alternate DNS Address**properly if needed.

5. Click **Save**.

8.2 Connect to Platform

Connect to the platform to upload files or apply information via the platform.

Before You Start

- Arrange the platform server.
- The communication between the dock station and server is normal.

Steps

Note

If you enable the platform connection, ISUP connection will be disabled automatically.

1. Go to **Network Settings → Platform Settings** .

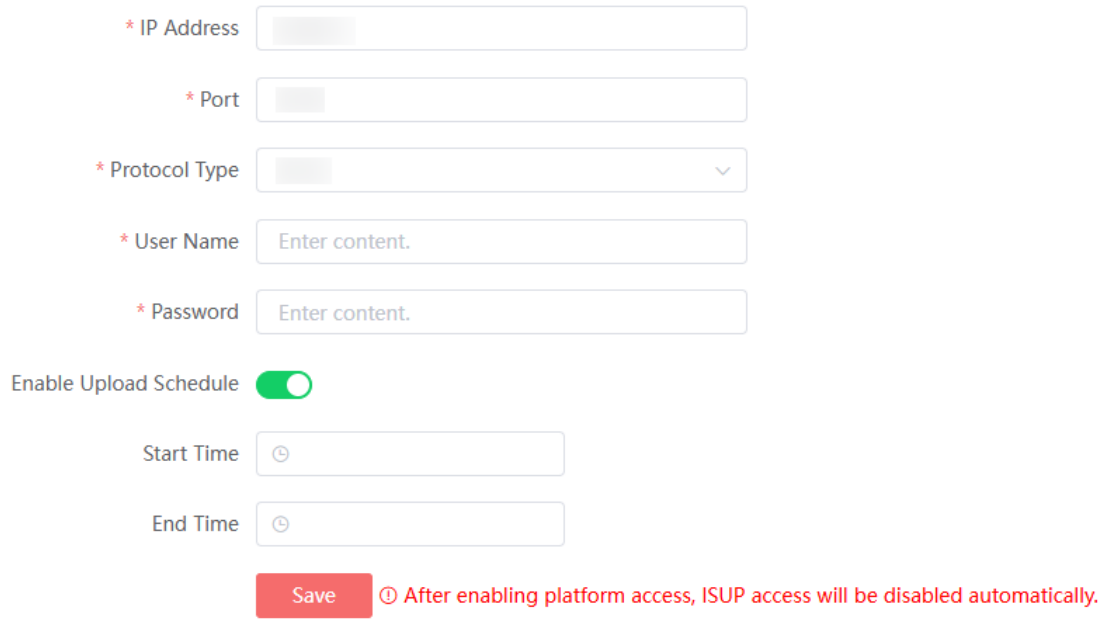


Figure 8-2 Connect to Platform

2. Enter **IP Address** and **Port** of the platform server.
3. Select **Protocol Type**.

9533

Connect the dock station to the platform via 9533 protocol which supports data exchange between the dock station and the monitoring center.

ISAPI

Connect the dock station to the platform via ISAPI protocol.

none

Disable platform connection.

4. Enter **User Name** and **Password**.
5. **Optional:** Enable upload schedule and set **Start Time** and **End Time** to upload files in a fixed time period.

Note

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

6. Click **Save**.

What to do next

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

8.3 Connect to ISUP Platform

ISUP is a platform access protocol. The dock station can be remotely accessed via this platform.

Before You Start

- Create the device ID on ISUP platform.
- Ensure the device can communicate with the platform normally.

Steps

Note

If you enable the ISUP connection, platform connection will be disabled automatically.

1. Go to **Network Settings → ISUP** .
2. Enable the function.

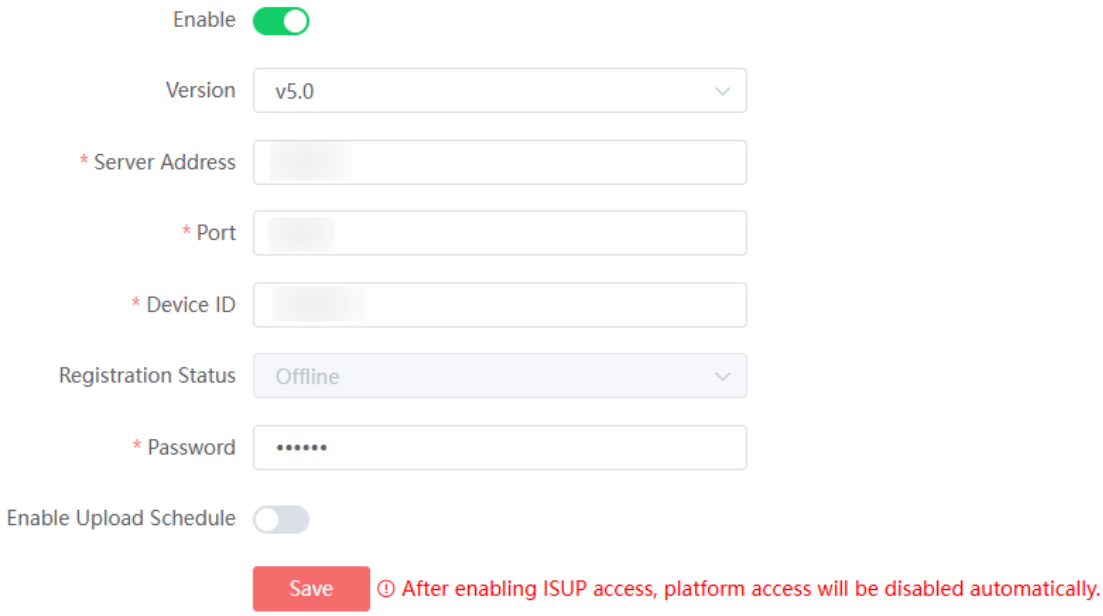


Figure 8-3 Connect to ISUP Platform

3. Select **Version**.
4. Enter **Sever Address**, **Port**, **Device ID**, and **Password**.
5. **Optional:** Enable upload schedule and set **Start Time** and **End Time** to upload files in a fixed time period.

Note

If this function is disabled, files will be uploaded to ISUP in real time.

6. Click **Save**.

What to do next

When the registration status is online, you can manage the device via the platform or server.

Chapter 9 System Settings

9.1 View Device Information

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

9.2 Synchronize Time

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

Steps

1. Go to **System → System Settings → Time Settings** .
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 set the device time manually. You can enable **Sync. with computer time** to synchronize the device time with that of the computer. Or set time manually.
   - 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**.

9.3 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**.

9.4 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. Enable HTTPS.
3. Click **Save**.

9.5 Connect to FTP

Set FTP parameters if you want to upload the collected files to the FTP server.

Before You Start

Set the FTP server, and ensure the device can communicate normally with the server.

Steps

1. Go to **System → System Settings → FTP** .

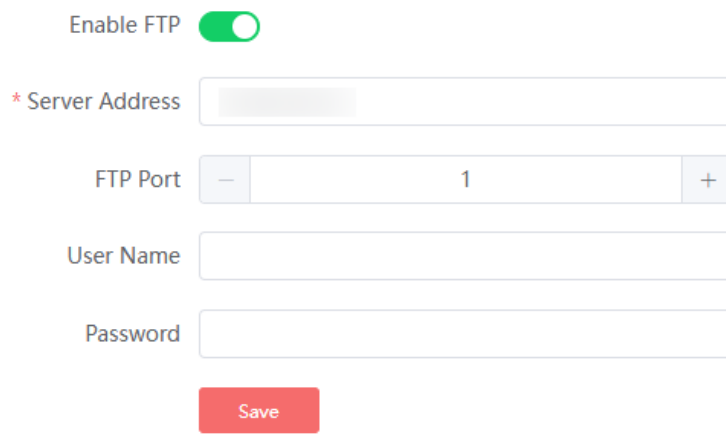


Figure 9-1 Connect to FTP

2. Enable FTP.
3. Enter **Sever Address**.
4. Select **FTP Port**.
5. Enter **User Name** and **Password**.
6. Click **Save**.

9.6 Upgrade Management

9.6.1 Upgrade via Platform

You can upgrade the dock station applied by the connected platform.

Before You Start
Connect the dock station to the platform.

Steps
1. Go to **System → System Settings → Upgrade Management → Upgrade via Platform** .
2. Click **Upgrade**, and the dock station will upgrade and reboot automatically.

Note

If **Upgrade** button is grey and cannot be operated, it means applying the program package from the platform failed.

9.6.2 Set Working Mode

You can select the dock station working mode, including to upgrade the connected body camera program applied by the connected platform, to collect the body camera files, and to detect the body camera software version and upgrade after the file collection completes.

Before You Start
Connect the dock station to the platform, and the platform has applied upgrade package of the body cameras to the dock station.

Steps
1. Go to **System → System Settings → Upgrade Management → Upgrade** .
2. Select **Upgrade Type** as **Body Camera**.
3. Select **Working Mode**.

Upgrade Mode

In this mode, the newly connected body cameras will start upgrade directly, and the body cameras of which the files are collecting will start upgrade after the file collection completes.

Collection Mode

After the body camera is connected, files will be collected automatically, and it will not be upgraded.

Compatible Mode

In this mode, after the body camera is connected, files will be collected first. After the collection completes, the dock station will detect if the software version of the body camera

is the newest. If not, the body camera will start upgrade. If the software version of the body camera is already the newest, it will keep the collection mode.

Note

Do not cut off the power or disconnect the network during the upgrade, or exception may occur.

9.7 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 Settings** .
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**.

9.8 Set Data Encryption

Set data encryption to encrypt the collected files from the body cameras to enhance security. After encryption, you need to use dedicated player and enter correct encryption key to play the collected files on the computer.

Steps

1. Go to **System → System Settings → Encryption Settings** .
2. Enable **Encryption**.

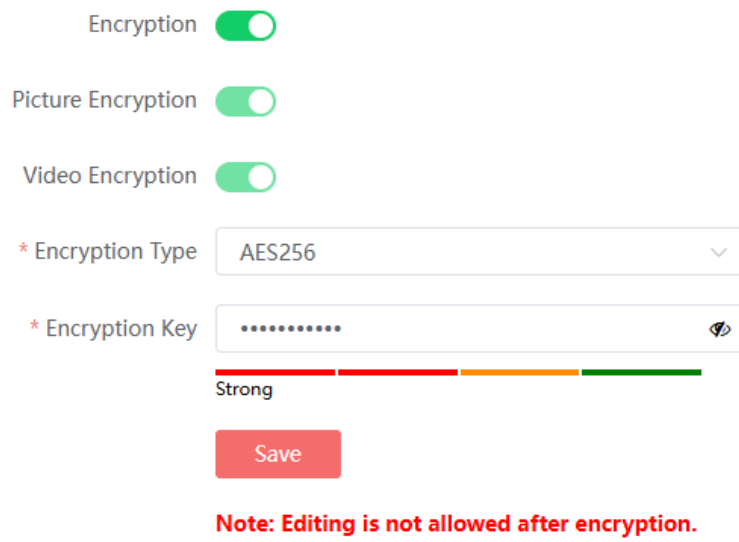


Figure 9-2 Set Data Encryption

3. Enable **Picture Encryption** or **Video Encryption**.

Note

After the functions are enabled, they cannot be disabled.

4. Select **Encryption Type**.
5. Enter **Encryption Key**.
6. Click **Save**.

Result

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

What to do next

Play the collected files via Hikvision player or other players with Hikvision play plugin. Visit Hikvision official website to download VSPlayer and install it. Or visit Hikvision official website to download MFPlugin and install it. Open the player and enter the set encryption key to play the files on the computer.

9.9 Activate Body Cameras in Batch

You can activate the inactive connected body cameras in batch via the dock station.

Steps

1. Go to **System → System Settings → Batch Activation** .
2. Enable the function.
3. Enter the body camera password, and confirm the password.
4. **Optional:** Set **Hotspot Password** and confirm the password.

5. Click **Save**.

What to do next
After activation, use the activation password to log in to the body camera to operate.

9.10 Change Admin Password

You are recommended to change the dock station admin password regularly to enhance data security.

Steps
1. Click **admin** on the upper right corner of the interface, and click **Change Password**.
2. Enter **Old Password**.
3. Enter **New Password** and confirm it.
4. Click **OK**.

What to do next
Next time you log in to the dock station, use the new password.

Chapter 10 System Maintenance

10.1 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.

10.2 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 → Device Maintenance** .
2. Click **Reboot**.
3. Click **OK**.

10.3 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 → Device Maintenance** .
2. Select the restoration mode.
   - Click **Restore Default Settings** and enter the admin password to restore the parameters except the IP parameters and user parameters to the default settings.
   - Click **Restore all parameters** and enter the admin password to restore all the parameters to the factory settings.
3. Click **OK**.

10.4 Export Configuration Parameters

You can export the configuration 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.

10.5 Export Debug Log

The technicians can export the debug log to troubleshoot and maintain the device.

Steps

1. Go to **System → System Maintenance → Exporting Debugging Log** .
2. Enable **Log saving**, and click **OK**.

   The device will save the debug log automatically.
3. Click **Export** and click **OK** to export the debug log to the computer.

10.6 Import Configuration 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 select the configuration file.
3. Click **Import**.

Result

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

10.7 Upgrade Device

Upgrade the dock station 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** to select the upgrade file.
3. Click **Upgrade**.

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

10.8 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 Database** .
2. Click **Format**.
3. Enter the admin password on the popup window.
4. Click **OK**.

10.9 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**.

10.10 Set Local Mode

Enable local mode to add body cameras and persons.

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


See Far, Go Further