HIKVISION°

DS-MDS003

Dock Station
User Manual

© 2021 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 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 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 INSPECTION, 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 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
DANIOED	Indicates a hazardous situation which, if not avoided, will or could result in death or
DANGER:	serious injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in
CAUTION:	equipment damage, data loss, performance degradation, or unexpected results.
NOTE	Provides additional information to emphasize or supplement important points of the
NOTE:	main text.

Safety Instruction

Laws and Regulations

Use of the product must be in strict compliance with the local laws and regulations. Please shut down the device in prohibited area.

Network

Please enforce protection for personal information and data security as the device may be confronted with network security problems when it is connected to the Internet. Please contact us if the device might face network security risks.

Understand that you have the responsibility to configure all the passwords and other security settings about the device, and keep your user name and password.

Data

DO NOT disconnect the power during formatting, uploading, and downloading, or files may be damaged.

Contents

Chapter 1	Intro	oduction	6	
1.1	Prod	luct Introduction	6	
1.2	. Key F	Features	6	
Chapter 2	Start	tup	7	
2.1	Activ	vation	7	
2.2	. Home	e Page Overview	7	
Chapter 3	Basi	c Operation	9	
3.1	Conn	nect Device	9	
3.2	. Colle	ect File	9	
3.3	. Mana	age File	10	
	3.3.1	1. Authenticate Permission	10	
	3.3.2	2. Search File	11	
	3.3.3	3. Play and Edit File	12	
	3.3.4	4. Lock File	13	
	3.3.5	5. Upload File to Platform	14	
3.4	ı. Conn	nect to Platform	14	
3.5	. Mana	age Storage	15	
	3.5.1	1. Set Local Storage	15	
	3.5.2	2. Connect to Storage Server	15	
3.6	6. Mana	age Device	16	
3.7	7. Disconnect Device			
Chapter 4	Safe	ety Management	18	
4.1	Mana	age Person	18	
	4.1.1	1. Add Person	18	
	4.1.2	2. Collect Face Picture	19	
4.2	. Edit l	Password	20	
4.3	S. Set F	File Search Permission	20	
4.4	ı. Set F	Face Priority	20	
Chapter 5	Syst	em Configuration	22	
		<i>I</i> Basic Information		
5.2	. Set L	Language	22	
	S. Set D	Debug Mode	22	
5.4	ı. Set C	Collection Format	22	

DS-MDS003 Dock Station User Manual

Chapter 6	Maintenance	. 24
-	Search Log	
	Upgrade	
	Format Database	
	Restore Host Parameters	
	Restore System to Factory Settings	

Chapter 1 Introduction

1.1. Product Introduction

The Hikvision DS-MDS003 Dock Station, integrated with the Digital Evidence Management System (hereinafter referred to as software), provides an easy way to access body cameras, and collect, store, and play audio and video files in the connected body cameras via the software. You can associate user accounts with body cameras, search data collection records, and upload data via the software.

1.2. Key Features

- Highly stable dual system design supports wall mounting, mobile mounting, and desktop mounting.
- Ultra-large touchscreen with high resolution and convenient operation.
- Unlocks body camera bin by recognizing face to guarantee safe storage.
- Equipped with multiple body camera bins. Multiple dock stations can be connected.
- Auto charge body cameras.
- Standard USB interfaces connect to a keyboard or mouse for software operation, or connect to a USB flash disk to upgrade the dock station.
- Auto upload body camera data (picture, video, and audio), and clear the body cameras' storage space automatically.
- Locks important data to avoid deletion.
- Data protection when power is suddenly cut off.
- Log management to record all operation logs.
- Overwritten storage overwrites the collected data according to the collection sequence when storage is full.
- ANR uploads data to prevent data loss.
- File search in multiple modes, and video, audio, and picture playback.
- Local upgrade.
- Multi-user management. Multi-users can be associated with one dock station.
- Files can be uploaded to CVR and cloud storage.

Chapter 2 Startup

2.1. Activation

After the device starts, the screen will show the software activation page automatically. For the first access, you need to activate the device by setting an admin password. No operation is allowed before activation.

Steps

- 1. Select Start Configuration.
- 2. Select language.

NOTE: Select **Next** according to prompt after each step.

3. Set admin password.



STRONG PASSWORD RECOMMENDED — We highly recommend that you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

- 4. View the local storage.
- 5. Optional: Set platform parameters.
- 6. Select **Save** to finish the activation.

2.2. Home Page Overview

You will enter the home page of the software after activation.

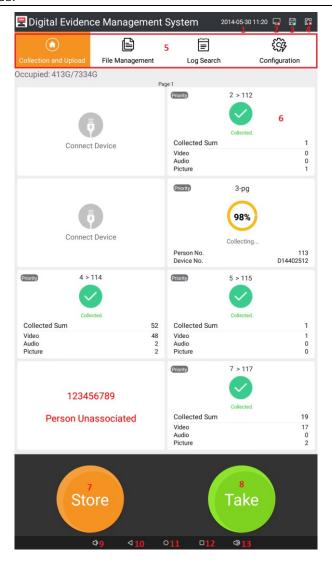


Figure 2-1 Home Page

No.	Description
1	Date and time
2	Platform connection status (after you set the platform parameters, it will appear)
3	Storage status
4	Network status
5	Main menu, including Collection and Upload, File Management, Log Search, and Configuration
6	Shows file collection status, number of collected files, and associated person information of the
	connected body camera
7	Select to open storage bin and connect the body camera (see "ConnectDevice" for details)
8	Select to open storage bin and disconnect the body camera (see "DisconnectDevice" for details)
9	Decrease the volume
10	Return to the former menu
11	The icon is disabled
12	The icon is disabled
13	Increase the volume

Chapter 3 Basic Operation

3.1. Connect Device

Connect body camera to the dock station before file collection.

Steps

1. On the Collection and Upload page, select Store, and the free body camera bin will open automatically.

NOTE: The free body camera bin will open from left to right, and from top to bottom in sequence.

- 2. Connect the mini USB interface in the bin to the USB interface of the body camera.
- 3. Place the body camera in the bin, and close the door.

Result

The body camera will be added to the software automatically after it is connected.

3.2. Collect File

After the body camera is connected, the software will start collecting files automatically.

Person Unassociated Body Camera

For a first-time connected body camera, the default device no. and "Person Unassociated" prompt will show on the corresponding bin of the software page. Associate person to the body camera first, or file collection will not start. Refer to "Manage Device" for details.

123456789 Person Unassociated

Figure 1, Person Unassociated

Person Associated Body Camera

After associating a person with the body camera, the software will start collecting files. During the collection process, you can view the person no., device no., person name, and collection status.

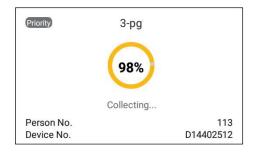


Figure 2, Collecting Files

Prior Collection

During the collection process, select **Priority** on the upper left corner of the body camera bin to enable prior collection. File collection of other body camera(s) will stop until the priority collection finishes.

NOTE:

If no body camera has enabled prior collection, the software will collect files from all the connected body cameras simultaneously.

During the prior collection process, select **Priority** again to disable the function.

Collection Finished

After file collection finishes, you can view **Collected Sum** and the number of collected **Video**, **Audio**, and **Picture** respectively. Select the body camera bin, and you can view **Person Name**, **Person No.**, and **Device No.**



Figure 3, Files Collected

3.3. Manage File

Admin user and persons with super admin permission can view and manage the files collected from all the connected body cameras. Persons without super admin permission can only view and manage the files collected from the associated body camera.

3.3.1. Authenticate Permission

Before you manage the collected files, authenticate permission to guarantee file security.

Before You Start

- Add person information, or collect face picture. Refer to "Manage Person" for details.
- Associate person to body camera. Refer to "Manage Device" for details.

Steps

- 1. Select File Management.
- 2. Authenticate permission.

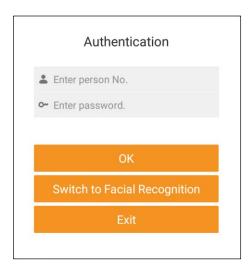


Figure 4, Authentication

- Authenticate via Associated Person Information
 - 1) Enter person no. and password.
 - 2) Select OK.
- Authenticate via Facial Recognition
 - 1) Select Switch to Facial Recognition.
 - 2) Adjust your face position in the collection area until your face is surrounded by a white rectangle. The host camera will capture the face picture automatically and compare it with the one collected when adding the person.

NOTE: If you enter the correct person information, or pass facial recognition, you can manage files.

Permission authentication is enabled by default. You can disable the function, but you are not recommended to disable the function. Refer to "Set File Search Permission" for details.

If you enable face priority, when you select **File Management**, the face picture collection window will pop up directly to authenticate your permission via facial recognition.

3.3.2. Search File

You can search files collected from body camera.

Steps

- 1. On the **File Management** page, set search conditions such as keywords, date, file type, etc.
- 2. Select Search.

Result

Searched results will be displayed in the list. View file thumbnails, file name, and file status.

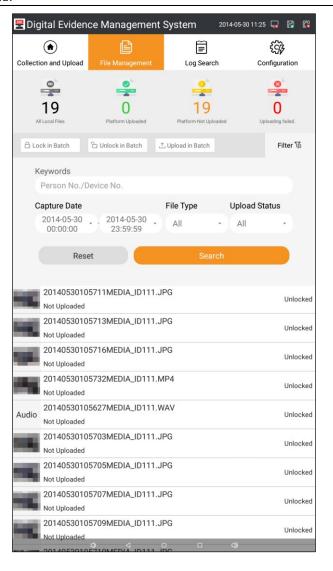


Figure 5, File Management

3.3.3. Play and Edit File

You can play the searched file, or edit remarks.

Steps

- 1. Search file.
- 2. Select a file to play.

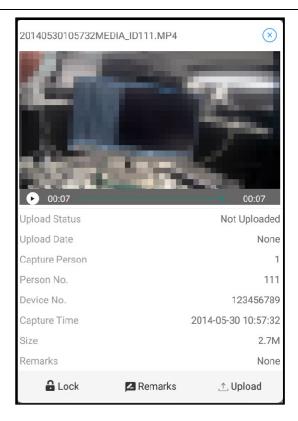


Figure 6, Play File

- 3. View the file information such as upload status, person no., device no., capture time, etc.
- 4. Optional: Select **Remarks** to edit file remarks, and select **Save** to save the remarks.

3.3.4. Lock File

You can lock important files to prevent it from being covered.

Steps

- 1. Search file.
- 2. Lock file.
 - Lock Single File
 - 1) Select a file to play.
 - 2) Select Lock to lock it.
 - Lock Files in Batch
 - 1) Select Lock in Batch to lock all the searched files.

NOTE: Select **Unlock** to unlock a single file in the play page, or select **Unlock in Batch** to unlock all the searched files.

Result

Locked files will be marked as "Locked" in the list, and they cannot be covered.

3.3.5. Upload File to Platform

You can upload file to platform.

Before You Start

- Connect to the platform server. Refer to "Connect to Platform" for details.
- The software communicates normally with the platform server.

Steps

- 1. Search file.
- 2. Upload file to platform.
 - Upload Single File
 - 1) Select a file to play.
 - 2) Select **Upload** to upload it to platform.
 - Upload Files in Batch
 - 1) Select **Upload in Batch** to upload all the searched files to platform.

Result

Uploaded files will be marked as "Platform Uploaded" in the list.

3.4. Connect to Platform

Set platform parameters before uploading the collected files to platform.

Before You Start

- Allocate the platform server.
- The software communicates normally with the platform server.

Steps

- 1. Select Configuration.
- 2. Enter admin password, and select **OK**.
 - **NOTE:** Every time you enter the **Configuration** page, you must enter the correct admin password to get the permission. Hereinafter it will not be illustrated any more.
- 3. Select Platform.
- 4. Select **Platform Type**.
- 5. Enter platform parameters, including IP Address, Port No., User Name, and Password.

6. Optional: To upload files at a specific time, enable upload schedule and set UploadTime.

NOTE: If upload schedule is disabled, the files will be uploaded to platform in real time.

7. Select OK.

Result

If platform connection succeeded, 😡 will appear on the upper right corner of the software page.

NOTE: If connection failed, check the platform parameters and network communication.

3.5. Manage Storage

3.5.1. Set Local Storage

You can edit and manage local storage.

Steps

- 1. Go to Configuration \rightarrow Basic.
- 2. View local storage information, including Total Space, Used Space, Free Space, and Usage.
- 3. Set Total Free Space and Clear Space.



CAUTION: The earliest data will be cleared according to time. Back up data in time to avoid data

loss.

Example: If you set **Total Free Space** as 10 GB, and set **Clear Space** as 5 GB, when the storage disk free space is less than or equal to 10 GB, 5 GB storage space will be cleared automatically.

- 4. Optional: After uploading the body camera data to the software, the data will be cleared automatically. If you do not want to clear the data automatically, disable **Clear Body Camera Data**.
- 5. Select **OK** to save the settings.

3.5.2. Connect to Storage Server

The storage server can store body camera files as expansion storage.

Before You Start

- Allocate the storage server.
- The software communicates normally with the storage server.

Steps

- 1. Go to the Configuration \rightarrow Storage.
- 2. Select **Storage Type** according to server type.
- 3. Enter server parameters, including **IP Address**, **Port No.**, etc.

NOTE:

Some server supports Bucket, AKEY, and other parameters. Keep the parameters the same with those of the server.

- 4. Optional: Enable **Auto Backup** if you want to upload body camera files to the storage server automatically.
- 5. Select **OK** to save the settings.

3.6. Manage Device

The connected body camera will be listed in the device list. The admin user can add, edit, and delete the body cameras.

Before You Start

- Connect the body camera to the dock station.
- Add person. Refer to "Add Person" for details.

Steps

- 1. Go to Configuration \rightarrow Device.
- 2. Select the added body camera.
- 3. Edit **Device Name**.
- 4. Select Associated Person.
 - 1) Check the person no. of a person or multiple persons.
 - 2) Select **OK** to associate the checked person(s) to the body camera.
 - 3) Select Save.

NOTE: One body camera can be associated with at most three persons. Each person can associate only one body camera.

- 5. Optional: Operate the following options.
 - **Delete:** Slide the added body camera item leftward, and select **Delete** to delete it.
 - Search: Enter search conditions, and select Search to search body camera information.

Export All

Select **Export All** to export the body camera information file to the connected USB flash disk when you need to set the same body camera information to another software.

Import

Connect the USB flash disk saved with the body camera information file to the host of a new dock station. On the new software, select Import to import the body camera information file.

3.7. Disconnect Device

After file collection, authenticate permission, disconnect your associated body camera, and take it away in time.

Steps

- 1. Select Collection and Upload.
- 2. Select **Take** to enter **Authentication** page.
- 3. Authenticate permission.
 - NOTE: You can authenticate via associated person information or facial recognition. Refer to step 2 of "Authenticate Permission" for details.
- 4. If you pass the authentication, the associated body camera bin will open automatically. Disconnect the body camera with the mini USB interface and take it away.
 - **NOTE:** If you forget your person no. or password, or fail to recognize the face, you can hold the corresponding bin on the software page and enter the admin password to open the body camera bin forcedly.

Chapter 4 Safety Management

4.1. Manage Person

To raise file security, you are recommended to distinguish persons' permissions to manage files and avoid multiple persons using one account to manage multiple body cameras.

4.1.1. Add Person

Add persons to manage body cameras.

Steps

- 1. Go to Configuration \rightarrow Person.
- Select Add.

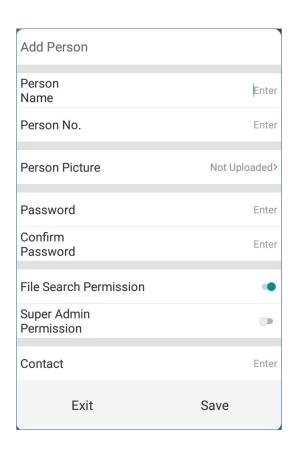


Figure 4-1 Add Person

3. Enter person information including Person Name, Person No., Password, and Contact.

NOTE: The password must be six-digits.

- 4. Optional: Select **Person Picture** to collect a face picture. Refer to "Collect Face Picture" for details.
- 5. 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 associated body camera.

- Super Admin Permission: If you enable this permission, the person can view and manage all files collected from all connected body cameras, no matter which body camera is associated with a person. If you disable this permission, the person can view and manage the files only collected from the body camera associated with him or her.
- 6. Select **Save** to save the settings.

NOTE: The added person will be listed on the page.

Up to 64 persons can be added.

- 7. Optional: Operate the following options.
 - Edit: Select the added person to edit the information.
 - **Delete:** Slide the added person item leftward, and select **Delete** to delete the added person.
 - Search: Enter search conditions, and select Search to search the person's information.
 - **Export:** Select **Export All** to export the person's information file to the connected USB flash disk when you need to set the same person information to another software.
 - **Import:** Connect the USB flash disk saved with the person's information file to the host of a new dock station. On the new software, select **Import** to import the person's information file.

NOTE: The Admin user can add, edit, and delete added persons. A person can edit only one's own information.

4.1.2. Collect Face Picture

You can collect the added person's face picture for permission authentication.

Steps

1. When you add a person, select **Person Picture** to enter the **Face Picture Collection** page.



Figure 7, Face Picture Collection

- 2. Adjust your face position until your face is surrounded by a white rectangle. The host camera will capture your face picture automatically and the confirmation window pops up.
- 3. Select **OK** to confirm the collected face picture.

Result

You can manage files by authenticating via facial recognition.

4.2. Edit Password

You can edit the software password regularly to enhance data security.

Steps

- 1. Go to Configuration \rightarrow Password.
- 2. Enter Old Password and New Password.



STRONG PASSWORD RECOMMENDED — We highly recommend that you create a strong password of your own choosing (using a minimum of eight characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. We also recommend that you reset your password regularly. Especially in high security systems, resetting the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

- 3. Confirm the password.
- 4. Select **OK** to save the settings.

4.3. Set File Search Permission

To raise file security, you are recommended to enable permission authentication for file management.

Steps

- 1. Go to Configuration \rightarrow Basic.
- 2. Enable File Search Permission.
- 3. Select **OK** to save the settings.

Result

You need to enter person no. and password, or recognize face to authenticate the permission for file management.

4.4. Set Face Priority

Enable face priority to recognize a face instead of authenticated person no. and password when you enter the **File Management** page or take the body camera.

Before You Start

Enable file search permission. Refer to "Set File Search Permission" for details.

Steps

- $1. \quad \text{Go to } \textbf{Configuration} \rightarrow \textbf{Basic}.$
- 2. Enable Face Priority.
- 3. Select **OK** to save the settings.

Result

Next time you enter the **File Management** page, or take the body camera, the face picture collection window will pop up to authenticate your permission via facial recognition.

Chapter 5 System Configuration

5.1. View Basic Information

You can view basic information such as dock station no., host version no., APP version no., etc.

Steps

- 1. Go to Configuration \rightarrow Basic.
- 2. View basic information, including Dock Station no., Host Version no., APP Version no., etc.

5.2. Set Language

You can select the system language.

Steps

- 1. Go to Configuration \rightarrow Basic.
- 2. Select Language.
- 3. Select **OK**.

5.3. Set Debug Mode

You can set USB flash disk mode or debug mode.

Steps

- 1. Go to Configuration \rightarrow Basic.
- 2. Select Debug Mode.
 - USB Flash Disk Mode: Only in this mode can the dock station collect files normally.
 - **Debug Mode**: This mode is for the software developer to debug the dock station. It is not recommended for normal operator use.
- 3. Select OK.

5.4. Set Collection Format

You can select the collection format of video, audio, and picture.

Steps

- 1. Go to Configuration \rightarrow Basic.
- 2. Select Video, Audio, or Picture to edit the collection format.
 - +: Add new format. Enter the format in the text field, and select **Save**.

- 💼: Delete the format.
- 3. Select OK.

Result

The software will collect files only in the set format.

Chapter 6 Maintenance

6.1. Search Log

You can search the software operation log to troubleshoot problems.

Steps

- 1. Select Log Search.
- Set search conditions.
- 3. Select **Search**. The log information will be displayed in the list.

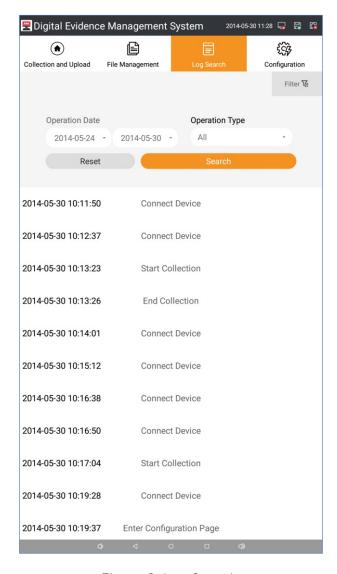


Figure 8, Log Search

- 4. Optional: Export log file.
 - 1) Connect a USB flash disk to the host USB 2.0 interface.
 - 2) Go to **Configuration** \rightarrow **Basic**.

3) Select **OK** of **Export Log File**. The log file will be exported to the connected USB flash disk.

6.2. Upgrade

You can upgrade the dock station APK, system, host, and all the dock station software.

Before You Start

Save the upgrade package (.zip format) in the root directory of the USB flash disk, and connect it to the host.

Steps

- 1. Go to Configuration \rightarrow Upgrade.
- 2. Select upgrade file.
 - Upgrade APK: To upgrade the application
 - **Upgrade System**: To upgrade the Android system
 - **Upgrade Host**: To upgrade the file collecting host
 - **Upgrade All**: To upgrade APK, system, and host simultaneously
 - 3. Select the upgrade package from the USB flash disk
 - 4. Select **OK** of **Enable Upgrade** to start upgrade

6.3. Format Database

To clear all the local data of the dock station, format the database.



CAUTION: The database will be cleared after formatting. Use this function with care.

Steps

- 1. Go to Configuration \rightarrow Basic.
- 2. Select **OK** of **Format Database**.
- 3. Select **OK** in the pop-up window.

Result

All the local data of the dock station are cleared.

6.4. Restore Host Parameters

You can restore the host parameters to the default settings.

Steps

1. Go to Configuration \rightarrow Basic.

- 2. Select **OK** of **Restore Host Parameters**.
- 3. Select **OK** in the pop-up window.

Result

The host parameters are restored to the default settings.

6.5. Restore System to Factory Settings

NOTE: You can restore the Android system to the factory settings.

Operate this function with care.

Steps

- 1. Go to Configuration \rightarrow Basic.
- 2. Select **OK** of **Restore System to Factory Settings**.
- 3. Select **OK** in the pop-up window.

Result

The Android system is restored to factory settings.



See Far, Go Further