

Evidence Manager 3.5

Administrator's Guide



Contents

Overview	4
Supported Devices.....	4
Installing and Setting Up Evidence Manager	5
Prerequisites for Installation.....	5
Installing Evidence Manager.....	6
Uninstalling Evidence Manager.....	7
Logging in to Evidence Manager.....	8
Using Templates.....	9
Adding Users.....	11
Modifying a User.....	12
Deleting a User Account.....	13
Updating Your Password.....	13
Configuring Evidence Manager	14
Setting up the SMTP Server.....	14
Configuring Evidence Manager for Discovery.....	15
Configuring the File Name Format.....	16
Configuring the Time Format.....	17
Setting the Stream Type.....	18
Managing Devices	19
Adding a Device to the Devices Folder.....	19
Managing MobileView Brand Devices.....	21
Running Diagnostics.....	29
Managing Docking Stations	33
Accessing Disk Analysis Data.....	34
Viewing and Changing Hard Drive Properties.....	36
Obtaining the HDD Log of a Docking Station.....	37
Accessing Disk Analysis Data.....	38

Support Information	40
Contact customer service.....	40
Product information.....	40
Warranty.....	40

Overview

Evidence Manager is a unified video management software platform capable of the following functions:

- Remote device management (including monitoring for device health)
- Video review (live and recorded)
- Evidence gathering and file generation

Evidence Manager requires a Windows computer for installation. It can be configured to work in an enterprise or a standalone environment.

Evidence Manager works with Depot Manager, which is a depot and device management software. To know more about Depot Manager, read the **Depot Manager User Guide**, available at <https://community.safefleet.net/>

TIP: Evidence Manager Terminology

On the Evidence Manager interface, the term **Devices** represents recorders. Therefore, as an example, the procedure **Changing Device Properties** actually refers to changing the properties of a recorder. Similarly, the term **Docking Stations** refers to caddies that contain hard drives (from recorders).

Supported Devices

Evidence Manager supports the following devices:

- TX8
- NX16
- H-series:
 - NH16 and NH16K
 - TH series: TH4C, TH4, TH6, and TH8
 - DH Series: DH4 and DH4C
- TL series: TL2, TL4, and TLHD
- DX Series: DX12 and DXHD
- MobileView III
- MobileView 3000 series: 3004, 3008, and 3012
- MobileView 7000 series: 7001 and 7001H

NOTE: Partial Support for Safe Fleet Recorders

At this moment, only MobileView devices, are discovered and listed under the **Devices** folder. Procedures described in the chapter **Managing MobileView Brand Devices** are only applicable to these devices. However, all devices can be managed following the procedures described in the chapter **Managing Docking Stations**.

Installing and Setting Up Evidence Manager

To install Evidence Manager, you must have administrator rights on the computer where you want to install Evidence Manager. We recommend that you install Evidence Manager only on a limited number of computers. Evidence Manager can be potentially used to export, an activity that you will want to ideally restrict to a need-only basis.

Prerequisites for Installation

Evidence Manager is typically installed on the same network as the Depot Manager server. The prerequisites for Evidence Manager are slightly different from the prerequisites for Depot Manager.

i NOTE: Minimum Free Disk Space

As noted in the table that follows, computers running Evidence Manager require a minimum of 500 GB disk space (1 TB preferred). However, we recommend that the computers have free disk space of 100 GB at any time. This is necessary for the export of multiple video files, or files large in size.

Requirement	Description	Additional Details
Hardware requirements		
System type	Business workstation	Needed for capabilities and warranties
Chassis	Mini tower or laptop	Needed for card slots or good graphic capability
Processor	i5 Dual/Quad Core minimum i7 Dual/Quad Core and later preferred	Needed for video decoding
Memory	4 GB minimum, 8-16 GB preferred	Needed for caching
Video card	1 GB video RAM, 2 GB and higher preferred	Needed for video playback
Monitor and resolution	1280x1024, 24 inches and greater preferred	Needed for application layout
Hard drive	500 GB, 1 TB preferred	Needed for local storage

Requirement	Description	Additional Details
CD/DVD optical drive	16x DVD +/- R or RW	Needed for evidence storing
Network adapter	1 Gigabit, such as 802.11a/b/g/n/ac Wireless Adapter	Needed for server or recorder connectivity
Sound card	On board	Needed for basic audio
Software requirements		
Operating system	<ul style="list-style-type: none"> • Microsoft Windows 7 • Microsoft Windows 10 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2016 	64-bit required
Software	.NET 4.0, MS C++ Redistributable Microsoft Visual Studio Redistributable	If not detected on your computer at the time of installation, the Evidence Manager executable will first install the missing software.

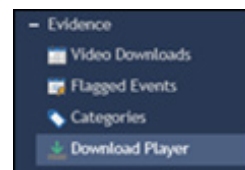
Installing Evidence Manager

1. Download the installer:

- **Using Evidence Manager with Depot Manager:** Log on to Depot Manager, and in the left pane, expand **Evidence**, and then click **Download Player**. Click **Download Now** in the center of the window.

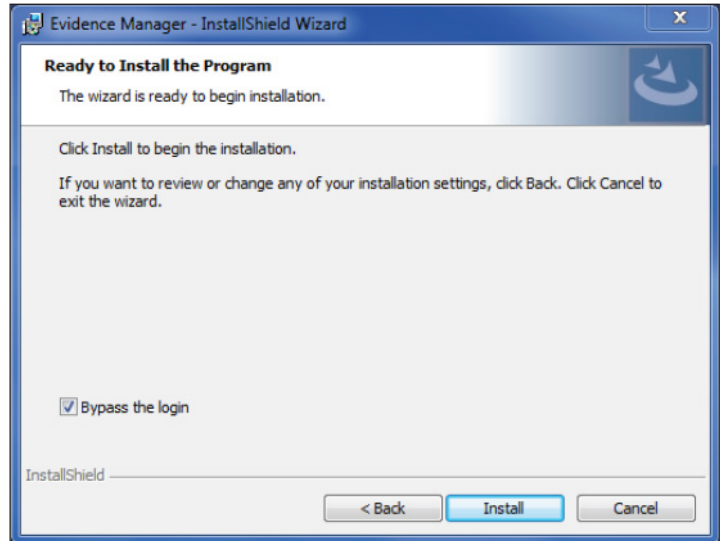
-OR-

Using Evidence Manager without Depot Manager: Download the installer from: <https://community.safefleet.net/sfpt/downloads/>



- On the computer where you want to install Evidence Manager, double-click this executable to open the installation wizard, and then click **Next**.

2. Accept the end-user license agreement by clicking **I accept the terms in the license agreement**, and then click **Next**.
3. Review the installation location, and click **Next**. If needed, change the installation location by clicking **Change**.
The default installation location is: *C:\Program Files (x86)\Safe Fleet\Depot Manager\Evidence Manager*
4. On the next step, select **Bypass the login** if you want to access Evidence Manager without credentials. If you would like to use a username/password combination while accessing Evidence Manager, DO NOT select this check box.
5. To begin the installation, click **Install** and click **Finish** once done.



i NOTE: Evidence Manager Licensing

The default Evidence Manager license is valid until December 31, 2022. It does not include Redaction, which requires a separate license.

To enable Redaction, follow the procedures described in the **Evidence Manager User Guide**.

Uninstalling Evidence Manager

If you no longer need to use Evidence Manager, you can uninstall it from your computer as you would any other software.

Windows 7, Windows Server 2012

1. From the Start menu, go to **Control Panel > Programs and Features**.
2. In the list of installed programs, click **Evidence Manager**, and click **Uninstall**.

Windows10

1. From the Start menu, go to **Settings > System**.
2. Click **Apps & features**.
3. Find and click **Evidence Manager** in the list of programs, and click **Uninstall**.

Logging in to Evidence Manager

If you selected to log in using credentials, and this is your first time logging in, use the default credentials:

- **User Name:** admin
- **Password:** admin

After logging in, you will be prompted to set a new password and select a security question.

i NOTE: Accessing Evidence Manager Without Credentials

If you opted to access Evidence Manager without credentials, only perform **steps 1** and **2**.

To log in to Evidence Manager:

1. From the **Start** menu, go to **All Programs > Safe Fleet**.
2. Click **Evidence Manager**.
-OR-
Double-click the **Evidence Manager** desktop shortcut.
3. If the **User Account Control** window appears, click **Yes** to proceed. The **Evidence Manager** login window appears.
4. (*First-time users*) Follow **steps 4 through 7**, and then go to **step 8**.
(*Returning users*) Skip to **step 8**.
5. Provide the default administrator credentials, and proceed with the installation.
6. Under **Change Challenge Response**, select a security question, and enter your answer.



i Note: Password Constraints

Your new password must be a minimum of 8 characters, and must include at least:

- 1 upper case and 1 lower case letter
- 1 number
- 1 of the following symbols:
~ ! @ # \$ % ^ + - =

7. Click **OK**. The **Evidence Manager** login window appears for you to log in with the new password.
8. Provide the login credentials:
 - **User Name**: The username for logging in
 - **Password**: The password for this user name

i NOTE: When Are Credentials Not Required?

If you selected **Bypass the login** while installing Evidence Manager, you do not need to provide your credentials while logging in.

9. Click **Login**.

Using Templates

Templates are preset formats that contain information related to the "look and feel" of Evidence Manager. Once you set the appearance of Evidence Manager to best suit your needs, you can save these preferences to a template. Whenever necessary, you can simply load one of the available templates to quickly customize the Evidence Manager UI.

Templates can contain:

- Information related to resizing and hiding the following panels: Device Manager, Map View, Metadata View, Bookmarks, and Metadata Player
- Information related to the layout, such as number of tiles, camera order, and overlay

Templates that are previously created are alphabetically arranged and available for loading for each instance of logging in.

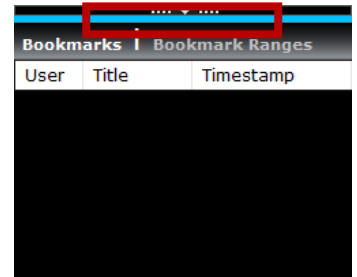
i NOTE: Who Can Access Templates?

Templates are associated with users. This means that if you log in to Evidence Manager using your credentials, the templates you create will be associated with your account, and available only for you to use. However, if you have opted to access Evidence Manager without credentials, then the templates are not associated with user accounts, and are therefore available for use by everyone, irrespective of who created them.

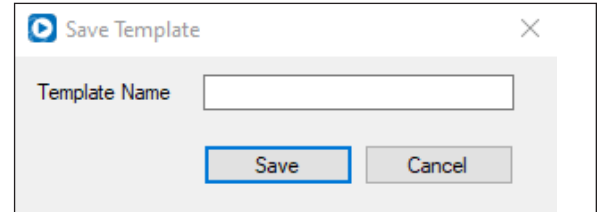
Creating a Template

1. Log in or open Evidence Manager.
2. Open a video file of your choice. For more information, see **Accessing Media from a Source of Your Choice** in the User Guide.
3. Make changes to the appearance. For more information, see **Setting a Preferred Layout** in the User Guide.

4. Hide the panels you feel aren't of use to you:
 - a. On the edges of the panel, look for a handlebar. The position of the handlebar, and the direction of the containing arrow will give you a sense of how the panel will be hidden.
 - b. Click the handlebar to hide the panel.



5. Go to **Templates** on the menu bar.
6. Click **Save Template As**, and on the **Save Template** window, provide a template name and save your changes.



Loading a Template

1. Log in or open Evidence Manager.
2. Open a video file of your choice. For more info, see **Accessing Media from a Source of Your Choice** in the User Guide
3. Go to **Templates** on the menu bar.
4. Click **Load Template**, and then click the template you want to apply.

The template is applied, and the appearance of the Evidence Manager UI changes in accordance with the template.

Deleting a Template

You can delete a template you no longer require. To do that, you must first load that template, and then delete it.

1. Log in or open Evidence Manager.
2. Load the template you want to delete, following instructions in ["Loading a Template" on page 10](#).
3. Go to **Templates** on the menu bar.
4. Click **Delete Current Template**.

The template is deleted from the list of templates saved in Evidence Manager.

Adding Users

If you are an administrator, you can add user accounts for accessing Evidence Manager. At the time of adding a user, you can also specify whether the user has administrator privileges. Generally, an administrator account has complete control over Evidence Manager. An ordinary user can perform most of the tasks that an administrator can, with the exception of user management and system administration.

User privileges

This table lists the privileges that an ordinary user and an administrator have.

Privilege	Administrator	User
Access video files	Yes	No
Manage users	Yes	No
Configure Evidence Manager	Yes	No
Manage passwords	Yes	Yes
Manage devices	Yes	Yes
Manage evidence	Yes	Yes

To add a user:

1. Log in to Evidence Manager.
2. Go to **Tools > User Management**.
OR
Click the User Management icon.
3. On the **User Management** window, click **Add User**.
4. On the **User Add** window, do the following:
 - a. **User Name**: Enter a username for this user.
 - b. **First Name**: Enter the first name of this user.
 - c. **Last Name**: Enter this user's last name.
 - d. **Email**: Enter the email address for this user.
 - e. **Phone Number**: Enter this user's phone number.
 - f. **Password**: Enter a password of your choice. Alternatively, set a system-generated password by clicking **Generate**.
 - g. **Permissions**: Select **Admin** to assign administrator privileges. Select **Active** to enable this user account.

5. Click **OK**.

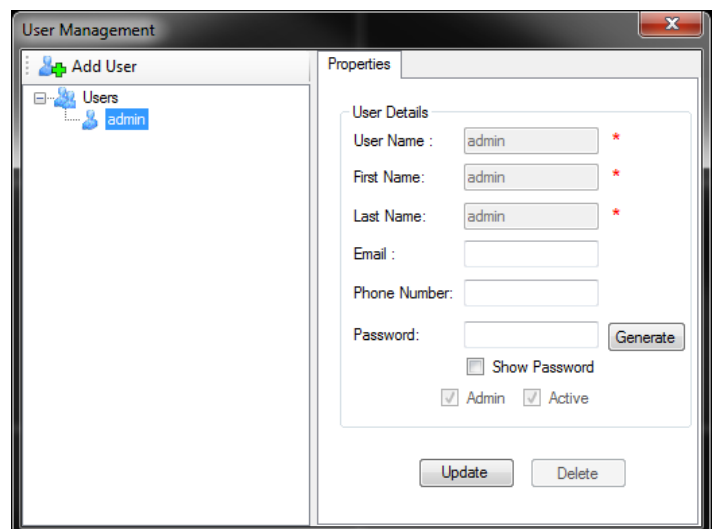
A user account is created for the user, who receives an email containing account details. Existing users receive email alerts indicating an account for a new user has been created.

Modifying a User

If you are an administrator, you can modify existing accounts of users who access Evidence Manager. You can also choose to enable or disable user accounts, and change user permissions.

To modify a user account:

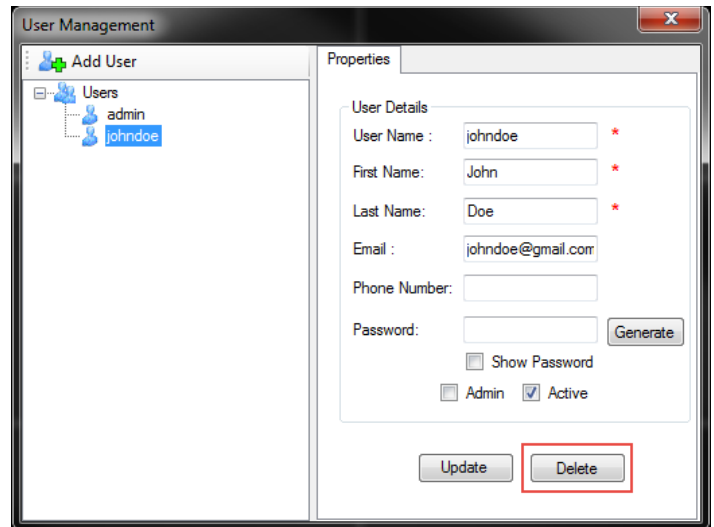
1. Log in to Evidence Manager.
2. Go to **Tools > User Management**.
OR
Click the User Management icon.
3. On the **User Management** window, click the user you want to update in the **Users** list to open **User Details** under **Properties**.
4. Do the following:
 - a. **User Name**: Enter the user name for accessing Evidence Manager.
 - b. **First Name**: Enter the first name of this user.
 - c. **Last Name**: Enter this user's last name.
 - d. **Email**: Enter the email address for this user.
 - e. **Phone Number**: Enter this user's phone number.
 - f. **Password**: Enter a password of your choice. Alternatively, use a system-generated password by clicking **Generate**.
 - g. **Permissions**: Select **Admin** to assign administrator privileges. Select **Active** to enable this user account.
5. Click **Update**.



The screenshot shows the 'User Management' application window. On the left, there is a tree view with 'Add User' and 'Users' folders. Under 'Users', a user named 'admin' is selected. The main area is titled 'Properties' and contains a 'User Details' section with the following fields: 'User Name' (admin), 'First Name' (admin), 'Last Name' (admin), 'Email', 'Phone Number', and 'Password'. The 'Password' field has a 'Generate' button next to it. Below the fields are checkboxes for 'Show Password', 'Admin', and 'Active'. At the bottom of the window are 'Update' and 'Delete' buttons.

Deleting a User Account

1. Log in to Evidence Manager.
2. Go to **Tools > User Management**.
OR
Click the User Management icon.
3. On the **User Management** window, click the user you want to delete in the **Users** list.
4. Under **Properties**, click **Delete**.

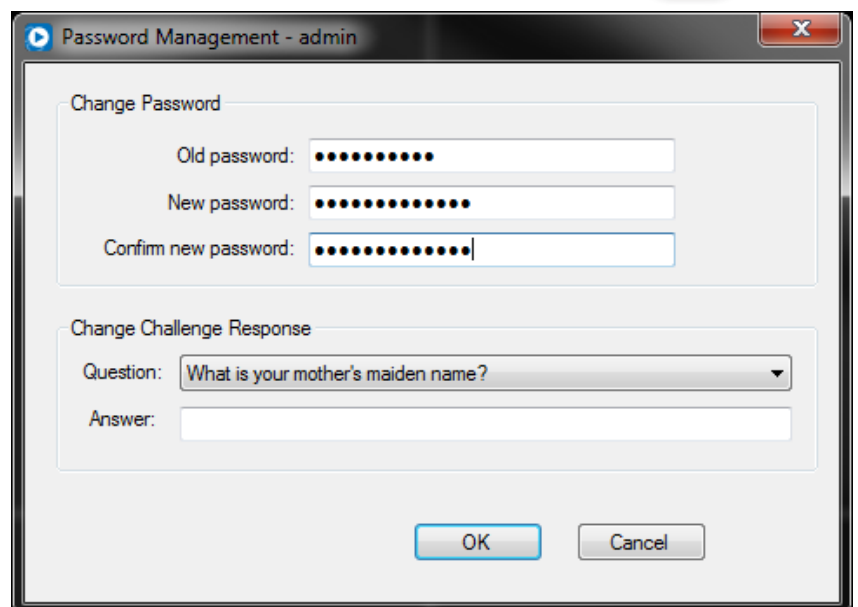
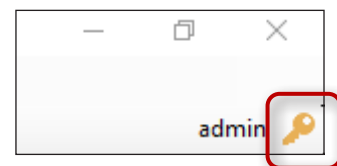


Updating Your Password

You can change your password at any time via the Password Management option. After you change your password, Evidence Manager sends to your email address an email notification that contains the details of the change.

To update your password:

1. Log in to Evidence Manager.
2. Go to **Tools > Password Management**.
OR
Click the **Password Management** icon in the upper right corner of the screen.
3. On the **Password Management** window, do the following:
 - a. **Old password:** Enter your old password.
 - b. **New password:** Enter a new password that you want to use for your account.
 - c. **Confirm new password:** Enter your new password again.
 - d. **Question:** Select a security question for your account.
 - e. **Answer:** Enter the answer to this question.
4. Click **OK**.



Configuring Evidence Manager

If you are an Evidence Manager administrator, you might be required to occasionally perform the following tasks:

- Configure Evidence Manager to discover devices
- Set up an email server for Evidence Manager
- Configure the file name format for download
- Configure the time format
- Configure a stream type for videos
- Configuring redaction properties

i NOTE: Redaction Settings

For information about configuring redaction properties, see **Redaction Settings** in the **Evidence Manager User Guide**.

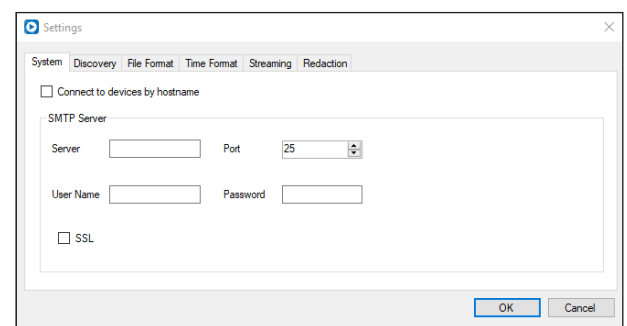
Setting up the SMTP Server

As an administrator, you can use the **Settings** option to set up an SMTP server for Evidence Manager. Once the SMTP server is configured, Evidence Manager communicates with this SMTP server over the default port 25 to send emails to intended recipients in the following situations:

- A new user account is created
- An existing user account is modified
- The configuration of a device using a configuration file either completes or fails
- An upgrade of the device either completes or fails

To set up the SMTP server:

1. Log in to Evidence Manager.
2. Go to **Tools > Settings**.
3. On the **Settings** window that appears, click the **System** tab.
4. Do the following:
 - a. **Connect to devices by hostname:** Select this checkbox to use the hostname of the SMTP server to connect to devices.
 - b. **Server:** If the previous check box is selected, enter the IP address or the hostname of the server.
 - c. **Port:** Enter or select the port that Evidence Manager will use while communicating with the SMTP server. The default value is 25.



- d. **Username:** Enter the username for accessing the SMTP server.
 - e. **Password:** Enter the password associated with this username.
 - f. **SSL:** Select this checkbox to enable the SSL protocol for communication between Evidence Manager and the SMTP server.
5. Click **OK**.

Configuring Evidence Manager for Discovery

Depot Manager, Evidence Manager, and multiple devices are connected over a network. At the time of deployment, your network administrator should have configured a network on which Depot Manager, Evidence Manager, and the devices can communicate.

By default, Evidence Manager uses the Multicast messaging protocol with 230.1.1.1 as the IP address. If necessary, you can choose another messaging protocol:

Unicast: Typically used when multiple networks are used with a router between the devices and the server. A unicast system involves one sender and one receiver, each with its own IP/network address. It is a one-to-one transmission from one point in the network to another point.

Multicast: Can only be used on flat networks where the server and devices share the same subnet, with no routers in between. Multicast is group communication where data transmission is simultaneously addressed to a group of destination computers. Multicast can be one-to-many or many-to-many distribution.

Broadcast: Broadcasting is the simultaneous transmission of a data packet to multiple network devices. Each network device receives all the signals sent by the transmitters. Security issues may arise during broadcasting and lead to data loss if a network is attacked by intruders. Used for smaller networks that do not support multicast or unicast.

For example, if you select the Multicast protocol:

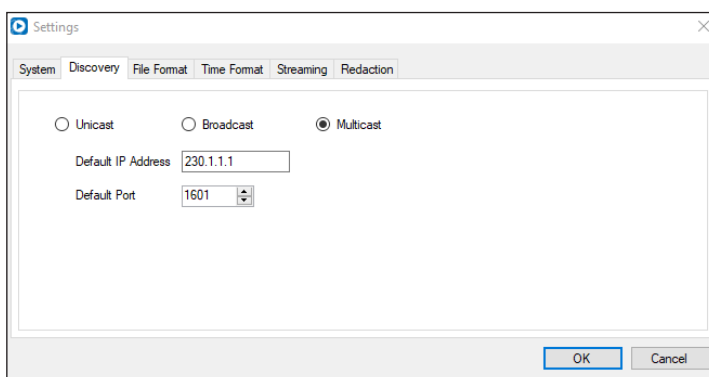
- Multiple instances of Evidence Manager appear under **Workstations**.
- Multiple devices that are discoverable appear under **Unknown Devices**.

i NOTE: Impact of Network Settings

Because system configuration has the potential to impact how Evidence Manager communicates, we recommend that you modify system settings only if you have a deeper understanding of the network configuration in your depot.

To configure Evidence Manager for discovery:

1. Log in to Evidence Manager.
2. Go to **Tools > Settings**.
3. On the **Settings** window that appears, click the **Discovery** tab.



4. Do the following:
 - a. Select the appropriate check box in order to specify a messaging protocol: **Unicast**, **Multicast**, or **Broadcast**.
 - b. **Default IP Address:** If you selected **Multicast**, then enter the IP address that will be assigned to this instance of Evidence Manager. The default value is 230.1.1.1, while the valid multicast range is: 224.0.0 to 239.255.255.255. If you selected **Broadcast**, Evidence Manager uses the default value of 255.255.255.255 as the IP address. This value cannot be changed.
If you selected **Unicast**, the Default IP Address box is grayed, and the IP address of this instance of Evidence Manager is set to match the IP address of the Depot Manager server. Evidence Manager will use the Default Port for communication.
 - c. **Default Port:** Type or select the default port that Evidence Manager will use for communication.
5. Click **OK**.

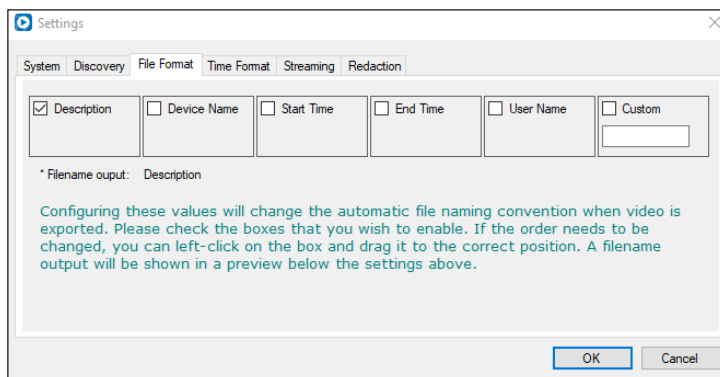
Configuring the File Name Format

When you export a media file, you can choose the destination where the media file is stored. At that time, you have the choice of giving the media file a name or have Evidence Manager automatically generate a name. For Evidence Manager to automatically generate a file name, there must be a file name format. This format is configured from the Settings menu.

You can select one or more of the following attributes that together will form the file name format: media file name, device name, start time, end time, user name, and a custom string. Evidence Manager uses an underscore (_) character to separate the chosen attributes, thus forming the file name. For example, if you choose the attributes file name and device name, an exported media file name might look like this: **CollisionIncident_Bus2020**.

To configure the file name format:

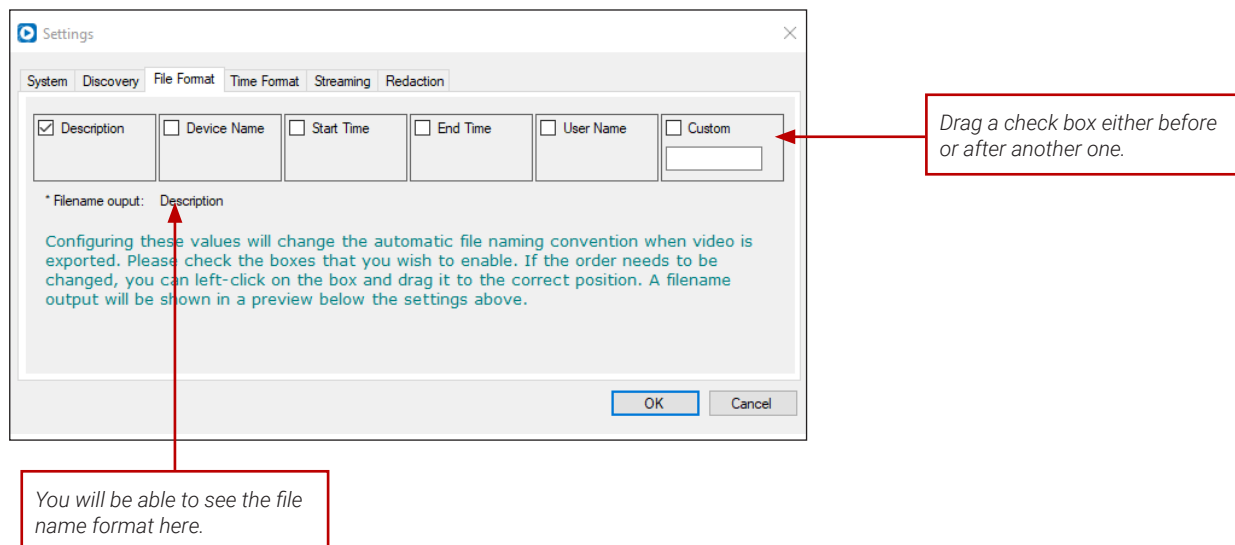
1. Log in to Evidence Manager.
2. Go to **Tools > Settings**.
3. On the **Settings** window, click the **File Format** tab.



i NOTE: Previous File Formats

If you selected a file name format previously, it will be replaced by the new format you select.

- Select the attributes you want as a part of your file name. For example, if you select **Device Name** and **End Time**, then whenever you export a media file, the media file will be saved with a name having the following format: **<Device Name_ End Time>**. The format output is available for preview below the check boxes.
- Click OK to apply the changes.



Changing the Order of the Attributes

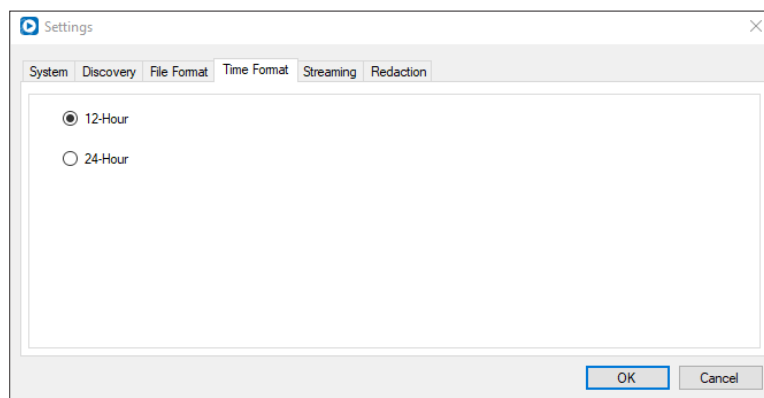
Left-click an attribute check box, and then drag it to the position you want to place it in. For example, from the file name format <Device Name_End Time>, if you want **End Time** to be positioned before **Device Name**, left-click the End Time box, and place it before the Device Name box.

Configuring the Time Format

You can set the format of the timestamp that is displayed on the media file as well as the camera tiles on which the media file is playing. The timestamp will also show on the media that you export, in the format you chose – 12-hour or 24-hour.

To configure the time format:

- Log in to Evidence Manager.
- Go to **Tools > Settings**.
- On the **Settings** window, click the **Time Format** tab.
- Select a time format: **12-Hour** or **24-Hour**.
- Click **OK**.



Setting the Stream Type

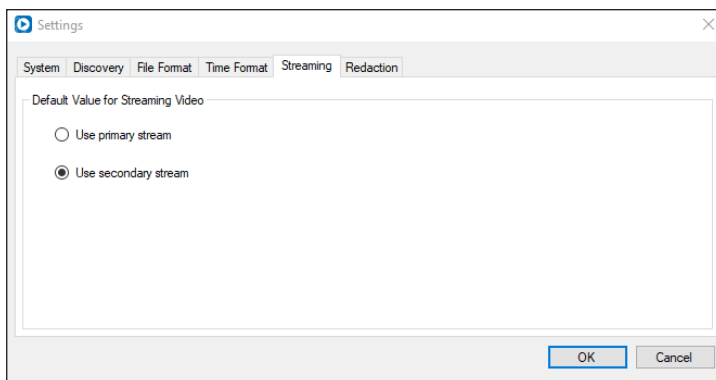
You can select a stream type for the videos that play from devices, as well as for the videos that are downloaded from devices. The stream type dictates the resolution of the video that plays. If you select Primary, the video plays with higher resolution, and is usually a larger file. If you select Secondary, the video plays with lower resolution, and is a smaller file.

i NOTE: What Videos are Affected by Stream Type

This setting only affects videos that are played or downloaded from MobileView recorders.

To select a stream:

1. Log in to Evidence Manager.
2. Go to **Tools > Settings**.
3. On the **Settings** window that appears, click the **Streaming** tab.



i NOTE: Videos Not Affected

The stream type is only set for videos that are directly accessed from devices. This setting will not reflect on videos that are stored on drives, workstations, or docking stations.

4. Under **Default Value for Streaming Video**, do one of the following:
 - To play higher resolution videos, select **Use primary stream**.
 - To play lower resolution videos, select **Use secondary stream**.
5. Click **OK**.

💡 TIP: Changing the Stream Type for Videos Already Playing

If a video is playing when you set a stream type, you must close the video, and open it again for the changes to reflect.

Managing Devices

Devices are recorders that are fitted inside vehicles, and are configured to communicate with Depot Manager and Evidence Manager via a network. Evidence Manager connects to devices to display either live or recorded videos. When Evidence Manager is opened in Standalone Mode, devices communicating on the same network are generally auto-discovered, and appear under **Unknown Devices**. You must associate such devices with Evidence Manager by organizing them under the **Devices** folder.

TIP: Evidence Manager Terminology

On the Evidence Manager interface, the term "Devices" represents recorders. Therefore, the topic "Managing MobileView Devices" contains procedures for managing recorders.

TIP: What Devices Can Be Added?

At this moment, only MobileView devices can be added to the **Devices** folder following the procedures "[Adding a Device to the Devices Folder](#)" on page 19 and "[Connecting to a Device Using the Service Port Feature](#)" on page 21.

Adding a Device to the Devices Folder

Evidence Manager normally auto-discovers devices connecting on the network. In some situations, Evidence Manager cannot auto-discover devices. An example of such a situation is when Evidence Manager and the devices are not on the same subnet, which prevents Evidence Manager from auto-discovering the device. These devices will have to be manually added. Another instance where manually adding a device is useful is when you do not have the connectivity for accessing a device, but you have its details handy. You can add this device to Evidence Manager, and when possible, connect to the device.

To better organize the devices under the **Devices** folder, you can create sub-folders inside the Devices folder, and then arrange devices inside each individual folder.

NOTE: How Imported Devices Are Indicated

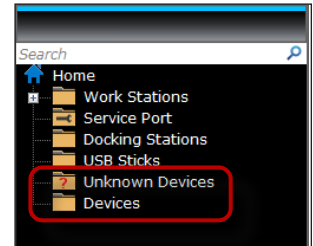
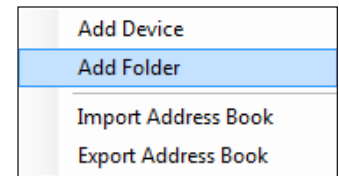
Devices imported into Evidence Manager will be listed under a folder having a prefix "Imported".

NOTE: How Many Devices Can Evidence Manager Connect To At A Time?

Multiple devices can appear under the **Devices** folder as a result of either auto-discovery or manual configuration. However, Evidence Manager can only connect to one device at a time.

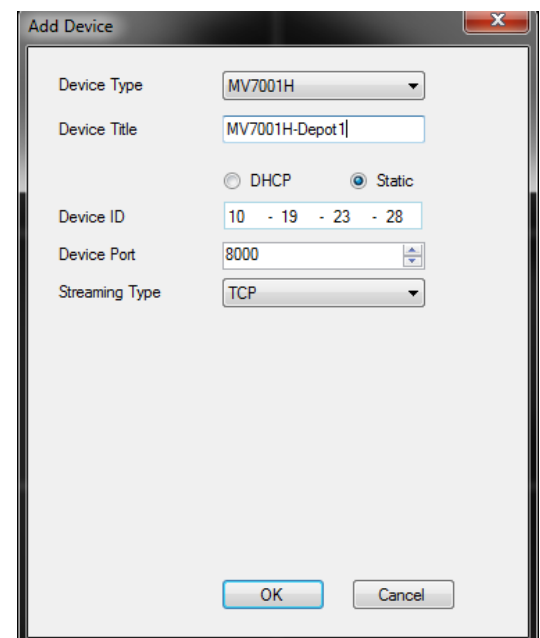
Adding an Auto-Discovered Device

1. Log in to Evidence Manager.
2. (Optional) Create a sub-folder under which you can organize devices:
 - a. Right-click Devices, and click **Add Folder**.
 - b. Enter a name for the folder. You can add multiple folders this way.
3. Add an auto-discovered device to the **Devices** folder:
 - a. Expand the **Unknown Devices** folder.
 - b. Click the device that you want to add to the Devices folder, drag it, and then drop it under **Devices**.



Manually Adding a Device

1. Under Device Manager in the left pane, right-click **Devices**, and then click **Add Device**.
OR
Go to **Tools > Address Book > Add Vehicle**.
2. On the **Add Device** window, provide the following:
 - **Device Type:** The type of the device from the list.
 - **Device Title:** The name for this device.
 - Type of IP address: **DHCP** for assigning dynamic IP addresses to this device. **Static** for entering a static IP address.
 - **Device ID:** Blank if you selected **DHCP**, else the IP address for this device.
 - **Device Port:** The port over which this device will communicate with Evidence Manager. The default value is 80.
 - **Streaming Type:** This value is set to TCP, and cannot be changed.
3. Click **OK**.



Managing MobileView Brand Devices

Connecting to a Device Using the Service Port Feature

Evidence Manager provides a way to view videos from devices by physically connecting the devices to a computer. The Service Port feature allows you to physically connect a device, and directly view videos stored in its hard drive.

To use the Service Port feature, first connect a device via its Service Port to the computer on which Evidence Manager is installed. Once that is done, add the device to Evidence Manager.

i NOTE: When Connecting a Device to a Computer

Make sure that you use a compatible cable to physically connect your device to the computer.

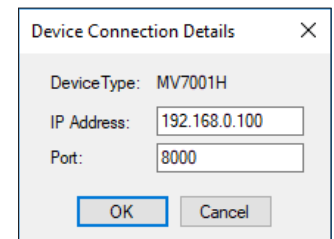
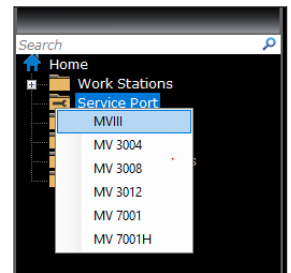
💡 TIP: Do Not Confuse Service Port Configuration Procedures

Connecting to a Device Using the Service Port Feature might look similar to Changing the IP Address of the Service Port of a Device Type. Although the steps are similar, the biggest difference is that when you add a device from the Service Port, the device is physically connected to your computer.

This is not the case when you change the IP address of the service port. Here, you only change the IP address without a physical connection.

To add a device from the Service Port:

1. Make sure you have the IP address and port number values for the device that you want to add.
2. Use the Service Port of the device to connect it to a computer on which Evidence Manager is installed. For instructions, see the recorder-specific guide at <https://community.safefleet.net/>
3. Log in to Evidence Manager.
4. Under **Home** 🏠, right-click **Service Port**, and click the device type that corresponds to your device. For example, MV7001H.
5. On the **Device Connections Details** window, confirm that the IP address and port number values match the corresponding values for this device.
6. Click **OK**. The device is added, and connected to Evidence Manager.



i NOTE: Clicking Service Port Is Not Working

After successfully adding a device, the capability of right-clicking **Service Port** is disabled, thus restricting connection to only one device at a time.

TIP: Device Behavior

Once connected, the device behaves exactly like a device that is added to the **Devices** folder. That is why you can perform any of the operations just as you would in the case of the device that appears under the **Devices** folder.

Changing Device Properties Using the Import/Export Feature

You can use the address book feature in Evidence Manager to change the properties of multiple devices in a bulk operation. The address book is a database of all the devices that are added in Evidence Manager. It also contains details such as device IP, username, password, port, and so on. The address book can be exported as a CSV file, which can in turn be used to populate another instance of Evidence Manager with a device list.

The following workflow explains how the Import/Export feature is used to change the properties of devices in a bulk operation:

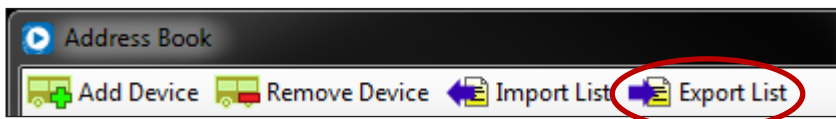
- Export the address book as a CSV file containing details such as mobile software version, device type, camera name, and so on.
- Modify the properties of devices, wherever needed, and save the file.
- Import this CSV file into Evidence Manager. This changes the properties of the devices.

NOTE: Using the Import/Export Feature

Use this feature to change device properties only if you are familiar with the fields typically contained in a device details file.

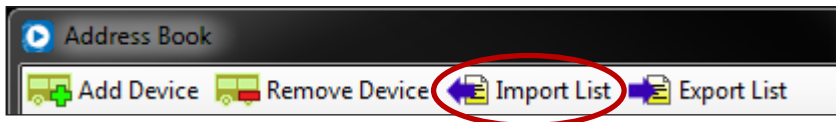
To change device properties using the import/export feature:

1. Log in to Evidence Manager.
2. Go to **Tools > Address Book**.
OR
Click the Address Book icon.
3. On the **Address Book** window, click **Export List**.

**Note: Another Method for Importing the Address Book**

You can also import the address book by right-clicking **Devices** and then clicking **Export Address Book**.

4. Browse to the location where you want to save this CSV file, and save this file.
5. Open the CSV file, make changes to the file, and save this file.
6. Go to **Tools > Address Book**.
OR
Click the Address Book icon.
7. On the **Address Book** window, click **Import List**.



NOTE: Another Method for Importing the Address Book

You can import the address book by right-clicking **Devices** and then clicking **Import Address Book**.

8. Browse to the location where the CSV is stored, select the CSV file you modified, and click **Open**.

The device details are imported and appear in a separate folder under Devices. This folder usually has a name with the prefix "Import".

Changing the IP Address of the Service Port of a Device Type


From Evidence Manager, you can change the IP address that a device uses for communicating via the Service Port. Once changed, all devices will use the newly set IP address specific to their type while communicating on the Service Port.

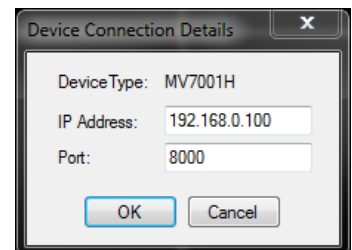
Keep in mind that for the purpose of device configuration, the Service Port is only used in the following circumstances:

- This is your first time connecting the device. The Rear Port is normally used for connecting a device to a computer. The default IP address of the Rear Port is 192.168.1.100, but you want to change this IP address from the Service Port.
- This is not your first time connecting the device to a computer, but you want to change the IP address on which the Rear Port can connect to a computer.

For more information about the use of Service Port and Rear Port, and their exact role in device configuration, see the recorder-specific guide available at: <https://community.safefleet.net/>

To set the IP address of devices:

1. Log in to Evidence Manager.
2. Under **Home** , right-click **Service Port**, and click the device type for which you want to change the IP address.
3. On the **Device Connections Details** window, enter a value for **IP Address** and **Port**.
4. Click **OK**.



The IP address for this device type is changed.

Using the On-screen Display to Configure a Device

Evidence Manager supports remote configuration of devices to which it can connect. Because maintenance teams no longer require physical access to devices in order to configure them, configuration becomes quicker, and the workload of the maintenance staff is reduced.

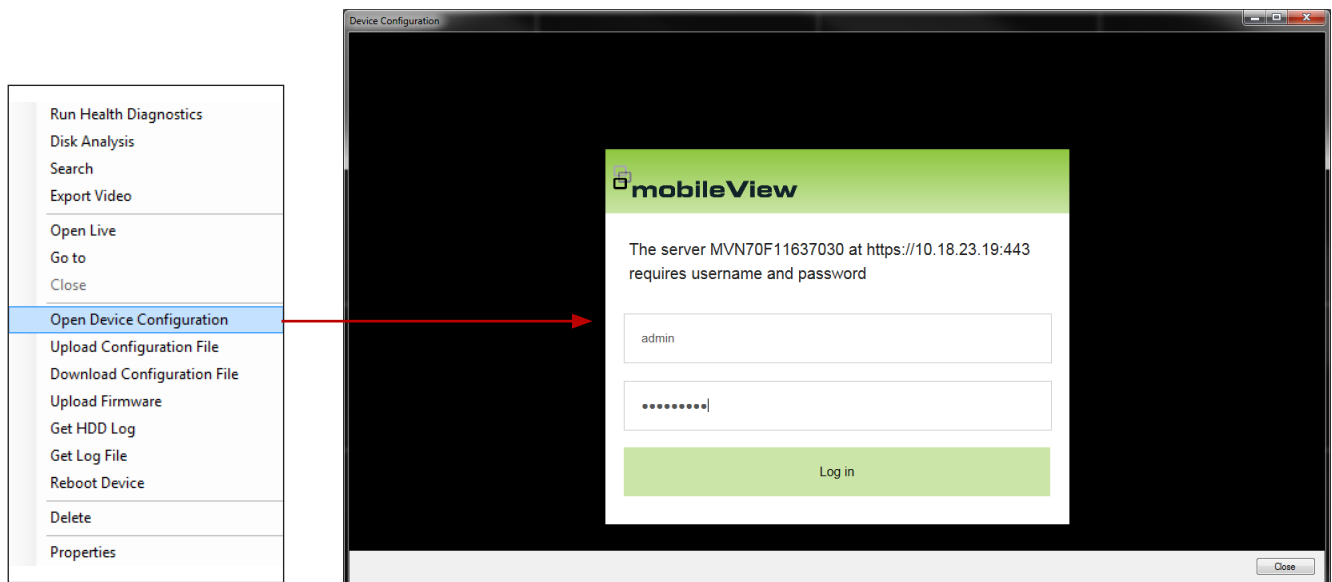
i NOTE: On-Screen Display Access

This procedure only describes how to access the on-screen display of a device. Once opened, use it just as you will when you physically connect the device to a computer.

If you upload the device firmware, the device appears offline until the upload completes.

To configure a device:

1. Log in to Evidence Manager.
2. Expand **Devices**, find the device you want to configure, and make sure it is connected.
3. Right-click this device, and click **Open Device Configuration**. A browser opens for accessing the on-screen display.



4. Enter the login credentials, and click **Log in**.
5. On the on-screen display, perform the configuration, following instructions in recorder-specific guides available at: <https://community.safefleet.net/>

Using the Configuration File to Configure a Device

Evidence Manager supports the use of configuration files to configure devices. A configuration file contains multiple types of configuration information, such as details about camera overlay configuration. Configuration files have the .cfg extension.

A configuration file can be used when:

- You have new devices that you want to configure the same as an existing device
- A device that was previously configured had to be repaired and you want to configure it again

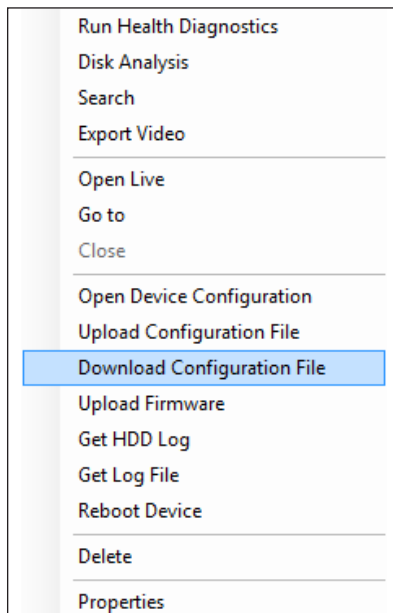
To use a configuration file to quickly configure a device, you must:

- Download the configuration file from a device, the properties of which you want to replicate
- Upload this file to the device you want to configure

Configuring a device this way is a one-time operation, which means that maintenance teams do not need to remember the configuration specifics. This reduces errors in configuration. Because configuration is initiated remotely, configuring devices becomes quicker.

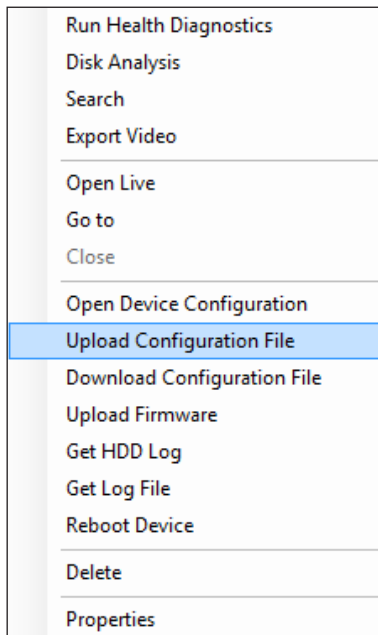
To download the configuration file of a device:

1. Log in to Evidence Manager.
2. Expand **Devices** under **Home** 🏠, find the device of your choice, and make sure that it is connected.
3. Right-click this device, and click **Download Configuration File**.



4. Browse to the location where you want to save the file, and click **Save**.

- Expand **Devices** under **Home** 🏠, find the device of your choice, and make sure that it is connected.
- Right-click this device, and click **Upload Configuration File**.



NOTE: Media Closes During Configuration

If videos are currently playing, Evidence Manager closes it before you can select the configuration file.

- Browse to the location of the configuration file that you previously saved, and select it.
- Click **Open**, and then **Upload**.

Changing Device Properties

You can change the general properties and the connection properties of a device from the **Properties** menu.

From here, you can view the capabilities of the device, and the details of the connected cameras. You can also add contact information of the maintenance personnel for quick reference.

To change device properties:

- Log in to Evidence Manager.
- Expand **Devices** under **Home** 🏠, find the device of your choice, and make sure that it is connected.
- Right-click this device, and click **Properties**. The **Properties** window appears.

4. Under **Connection**, do the following:
 - a. **Device Title:** Enter a name for this device.
 - b. Type of IP address: Select **DHCP** for dynamic IP addresses, or **Static** for a static IP address.
 - c. **Device ID:** If you selected **DHCP**, leave this blank. If you selected **Static**, enter the IP address for this device.
 - d. **Device Port:** Select a port over which this device will communicate. The default value is 80.
5. Under **Details**, do the following:
 - a. **Name:** Enter a name for the person who is in charge of maintaining this device.
 - b. **Phone:** Enter a phone number for this person.
 - c. **Street, City, State/Province, Zip/PostalCode, and Region/Country:** Use these fields to enter an address for this person.
 - d. **Notes:** Notes, if any.

i NOTE: Test Connectivity

To test device connectivity, click the **Test Connection** button.

The screenshot shows the 'Device Properties' dialog box with the 'Connection' tab selected. The fields are as follows:

- Device Type: MV7001H
- Device Title: MV7001--SeonSupport
- IP Configuration: DHCP, Static
- Device ID: 10 - 18 - 23 - 19
- Device Port: 8000
- Streaming Type: TCP

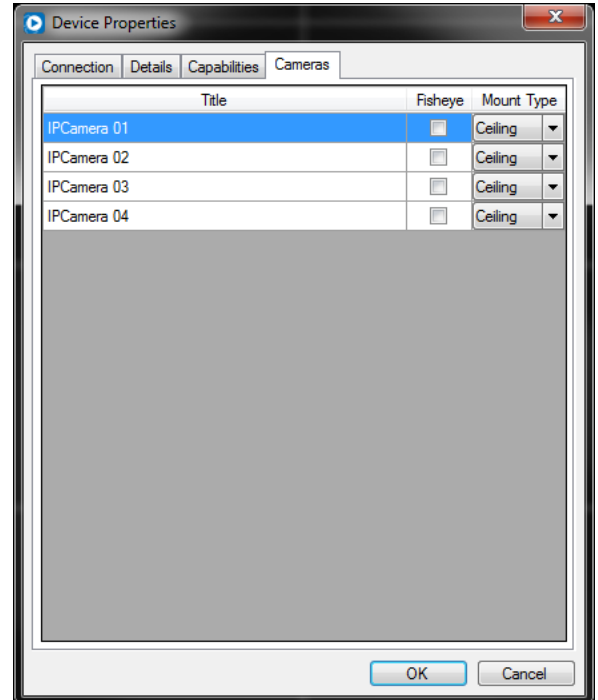
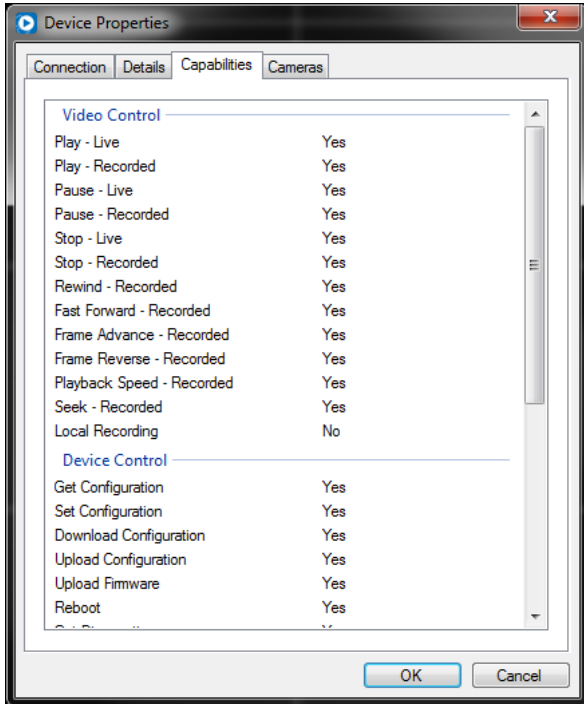
A 'Test Connection' button is located at the bottom of the dialog box. 'OK' and 'Cancel' buttons are at the bottom right.

The screenshot shows the 'Device Properties' dialog box with the 'Details' tab selected. The fields are as follows:

- Device Title: MV7001--SeonSupport
- Camera Count: 4
- Contact Info section:
 - Name: [text box]
 - Phone: [text box]
 - Street: [text box]
 - City: [text box]
 - State/Province: [text box]
 - Zip/PostalCode: [text box]
 - Region/Country: [text box]
- Notes: [text area]

'OK' and 'Cancel' buttons are at the bottom right.

6. Under **Capabilities**, view: Video Control, Device Control, Connection Types, and Other capabilities.
7. Under **Cameras**, view details such as camera name and mount type.
8. Click **OK**.



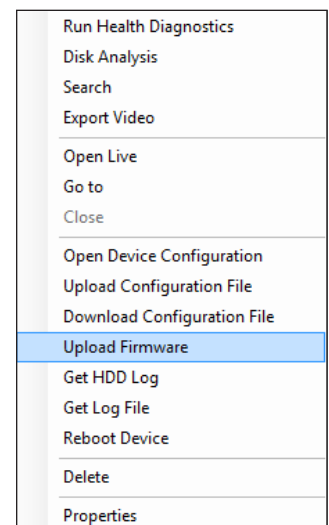
Uploading Device Firmware

You can use the firmware upload feature of Evidence Manager to upgrade to the most recent version of firmware on a device. Evidence Manager "pushes" the firmware file to the device, thereby initiating the firmware upgrade. Since the upload is initiated remotely, the need for maintenance staff to physically access the device is eliminated, thus making the upgrade simpler and faster.

To upload a device firmware:

1. Keep the firmware file (.bin) handy.
2. Log in to Evidence Manager.
3. Expand **Devices** under **Home** 🏠, find the device of your choice, and make sure that it is connected.
4. Right-click this device, then click **Upload Firmware**.
5. Browse to the location of the firmware file, select the file, and click **Open**.

The firmware upload starts, and a progress bar appears in the bottom-left corner of the Evidence Manager taskbar. During the process, the device stays offline.

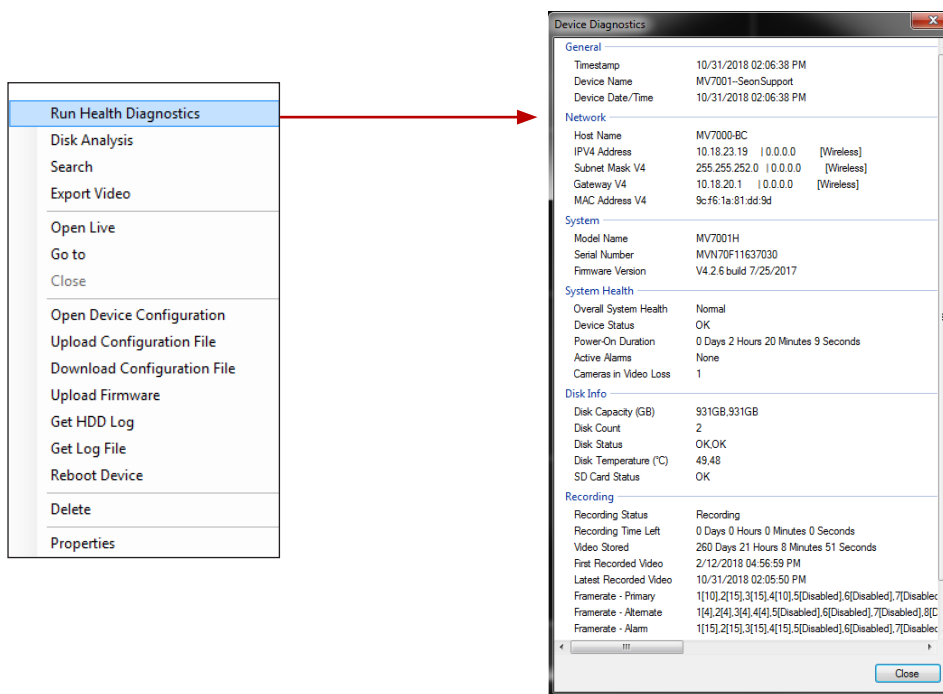


Running Diagnostics

Diagnostics is a health report of a device. It contains device details such as network information, system information, system health, and disk information. You can retrieve diagnostics of a device to which Evidence Manager is connected.

To run diagnostics:

1. Log in to Evidence Manager.
2. Expand **Devices** under **Home** 🏠, find the device of your choice, and make sure that it is connected.
3. (*TH and NH recorders only*) Right-click the recorder and click **Connect**.
4. Right-click this device, and click **Run Health Diagnostics**. Evidence Manager retrieves diagnostic information in a separate window.



NOTE: Addressing Issues Found by a Health Check


Evidence Manager only retrieves diagnostic data; if you encounter an issue with the device, you must correct that either from the on-screen display or Depot Manager, depending on the type of issue.

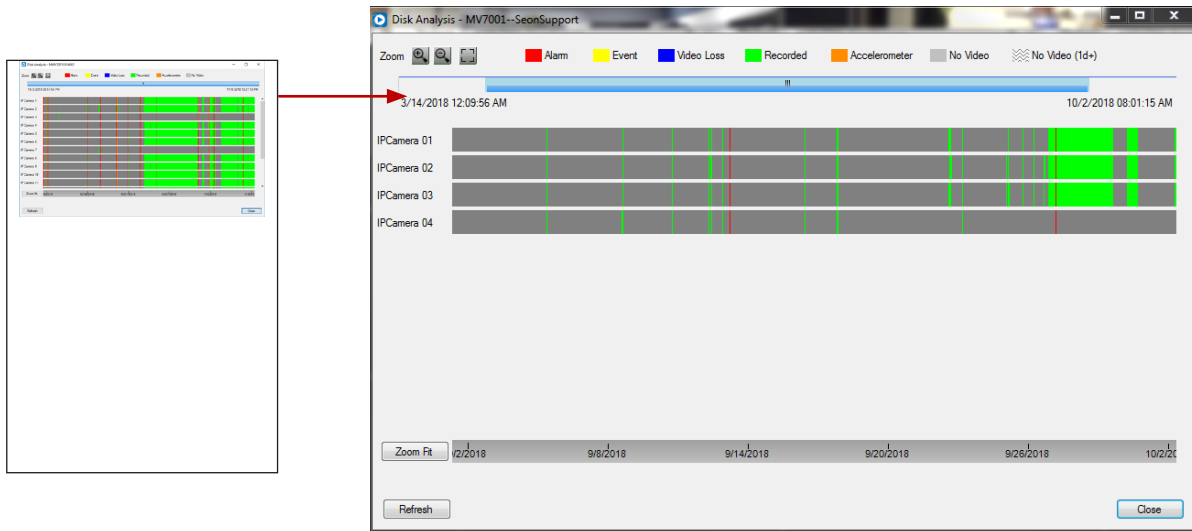
For troubleshooting tips, see either the recorder-specific guide or the Depot Manager guide, available at <https://community.safefleet.net/>

Viewing Disk Analysis Data

Disk analysis is a color-coded graphical representation of the type of data that is stored on a device's hard drive. It displays information such as total recorded video, alarms, events, video loss, and accelerometer data.

To view disk analysis data:

1. Log in to Evidence Manager.
2. Expand **Devices** under **Home**  in the left pane, find the device of your choice, and make sure that it is connected.
3. Right-click this device, and click **Disk Analysis**. Evidence Manager retrieves and displays the disk analysis data in the **Disk Analysis** window.



NOTE: If the Disk Analysis Fails

Sometimes, the disk analysis data might not appear the first time. If this happens, click the **Refresh** button to enable data display.

Understanding Disk Analysis Information

Use the legend at the top to get a sense of the type of data that this device contains.

Zooming In/Out of the Disk Analysis Information

Use the zoom controls in the top-left corner for zoom-in, zoom-out, and zoom-fit controls.

OR

Click **Zoom Fit** in the bottom-left corner for zoom-fit controls.

OR

Use the scroll wheel of your mouse to zoom in or zoom out of the video.

Playing Video From this Hard Drive

Double-click the graph at the point that represents the start time of the video. Periods with no video are displayed in gray.

Viewing the Most Recent Disk Analysis Data

Click **Refresh**.

Obtaining the HDD Log of a Device

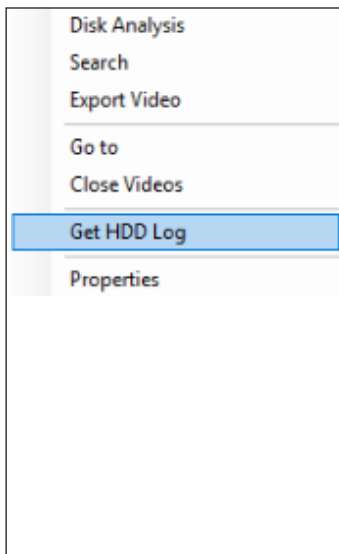
The HDD log is a log file of the hard drive of a device. It functions as a health report of the hard drive, and can be used to identify deviations from expected behavior.

The log file also comes handy while discussing issues with the Safe Fleet Technical Support team.

To obtain the HDD log:

1. Log in to Evidence Manager.
2. Expand **Devices** under **Home** 🏠, find the device of your choice, and make sure that it is connected.
3. Right-click this device, and click **Get HDD Log**.

The HDD log file is downloaded to your workstation.



Obtaining the Log File of a Device

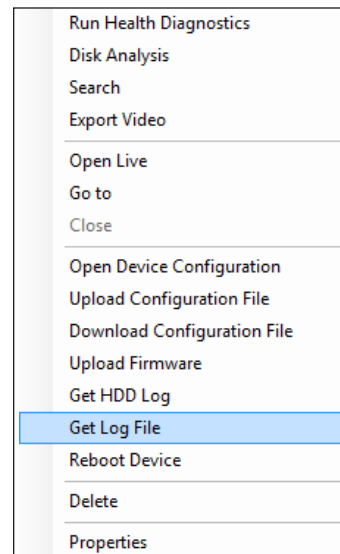
A device log file contains a list of all activities which are logged by a device.

Log files are used to gauge device health, identify issues, and generally ensure that the device is functioning as expected.

To obtain the device log:

1. Log in to Evidence Manager.
2. Expand **Devices** under **Home** 🏠, find the device of your choice, and make sure that it is connected.
3. Right-click this device, and click **Get Log File**.

The device log file is downloaded to your workstation.



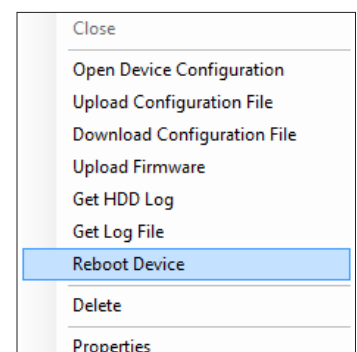
Rebooting a Device

You can initiate a device reboot remotely from Evidence Manager. A reboot might be necessary in certain situations. For example, after configuring a device, a reboot ensures that all the settings are applied correctly.

To reboot a device:

1. Log in to Evidence Manager.
2. Expand **Devices** under **Home** 🏠, find the device of your choice, and make sure that it is connected.
3. Right-click this device, and click **Reboot Device**.

As the device reboots, it will disconnect from Evidence Manager. After the reboot completes, the device will reconnect automatically.



Deleting a Device


When you delete a device, it disappears from the **Devices** folder, and is added to the **Unknown Devices** folder. Evidence Manager provides two different menu options for deleting devices; using either has the same result.

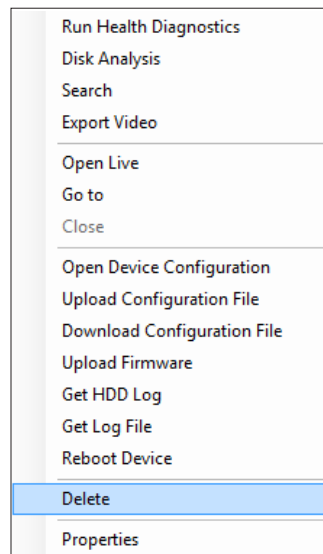
Deleting a Device via the Address Book

1. Log in to Evidence Manager.
2. Go to **Tools > Address Book**.
3. From the list of devices on the **Address Book** window, select the device you want to delete, and click **Remove Device**.
4. On the **Delete Device** window that appears, click **Yes** to complete the removal.



Deleting a Device via the Contextual Menu

1. Log in to Evidence Manager.
2. Expand **Devices** under **Home** , find the device of your choice, and make sure that it is connected.
3. Right-click this device, and click **Delete**. The device is deleted from the **Devices** folder.

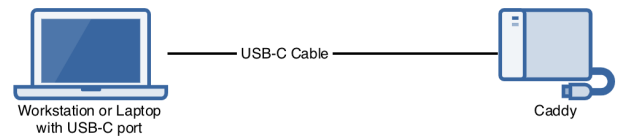
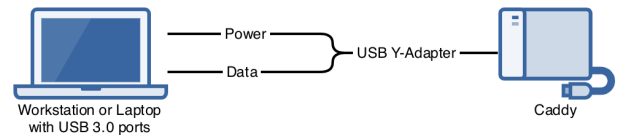
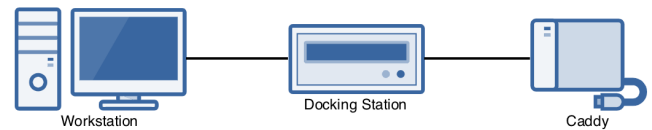


Managing Docking Stations

Docking stations allow a way to "dock" caddies to a computer or a network of computers. Hard drives inside caddies store videos recorded by the devices to which they belong. These videos can be accessed by physically connecting the caddy to a computer on which Evidence Manager is installed.

To do this, you can use:

- **A hardware docking station**
A hardware docking station provides a simple way of plugging a caddy to a computer. You must, however, use a compatible docking station. For information related to compatible hardware docking stations, contact the Safe Fleet Support Team.
- **Y-adapter**
A Y-adapter is needed for caddies containing two hard drives. The caddies need more power to read data from two hard drives, and the Y-adapter balances the power required. You must ensure that you have an approved Y-adapter.
- **USB-C cable**
A USB-C cable connection is necessary for computers that have a USB-C port. The USB-C cable ensures that there is enough power to read data from the hard drives within the caddies.



When a caddy connects to the network, Evidence Manager automatically detects it. Once detected, it appears under the **Docking Stations** folder. Inside this folder, the hard drive behaves similar to a device. For example, it has stored videos that you can play just like you would play videos from devices.

💡 TIP: Evidence Manager Terminology

In this topic, the term "docking station" can however, refer to the caddy, the USB-Y Adapter, or the USB-C cable to which compatible hard drives can be fitted.

📌 NOTE: Accessing Videos from Non-MobileView Recorders

Videos recorded by non-MobileView recorders (such as the H-series recorders) can ONLY be accessed using the Docking Stations feature.

💡 TIP: Docking Station Procedures

The Docking Station feature is the only way to access videos recorded by non-MobileView recorders. However, the procedures are applicable to MobileView recorders as well.

From a docking station, you can perform operations such as:

- Searching for videos using alarms and events
- Exporting videos
- Accessing disk analysis
- Searching for a video using the calendar
- Obtaining a HDD log
- Viewing docking stations properties

i NOTE: Searching and Exporting Media

The procedures for searching for and exporting videos are similar to the ones described in the topic **Managing Evidence** and are appropriate procedures for Users rather than Administrators. For more about searching and exporting media, please refer to the Evidence Manager User's Guide found in the Community.

Accessing Disk Analysis Data


Disk analysis is a color-coded graphical representation of the type of data that is stored on the hard drive within a docking station. It displays information such as total recorded video, alarms, events, video loss, and accelerometer data.

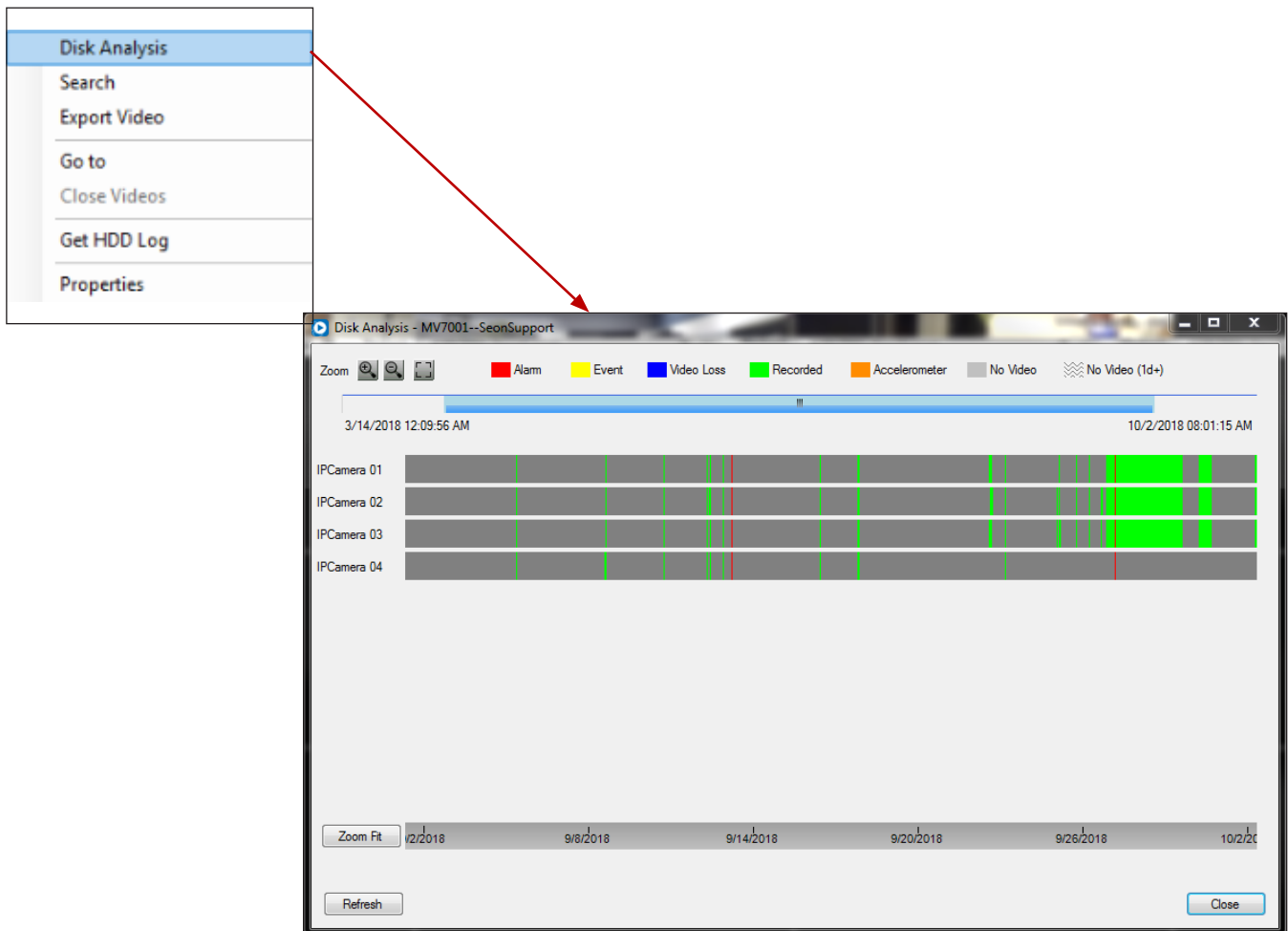
A docking station behaves similar to a device (recorder). That is why this procedure is exactly the same as the procedure described in the **Managing Devices** chapter.

i NOTE: Gray Periods on Disk Analysis

On a disk analysis display, periods where no video was recorded are displayed in gray.

To access disk analysis data:

1. Log in to Evidence Manager.
2. Expand **Docking Stations** under **Home**  in the left pane, and find the docking station of your choice.
3. Right-click this docking station, and click **Disk Analysis**. Evidence Manager retrieves and displays the disk analysis data in the **Disk Analysis** window.



Understanding Disk Analysis Information

Use the legend at the top to get a sense of the type of data that this device contains.

Zooming In/Out of the Disk Analysis Information

Use the zoom controls in the top-left corner for zoom-in, zoom-out, and zoom-fit controls.

OR

Click **Zoom Fit** in the bottom-left corner for zoom-fit controls.

OR

Use the scroll wheel of your mouse to zoom in or zoom out of the video.

Playing Video From this Hard Drive

Double-click the graph at the point that represents the start time of the video. Periods with no video are displayed in gray.

Viewing the Most Recent Disk Analysis Data

Click **Refresh**.


Viewing and Changing Hard Drive Properties

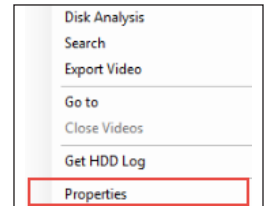
You can change the general properties of a hard drive from the **Properties** option. The Properties option also displays the following properties that are not editable: connection details, capabilities, and camera details of a hard drive.

NOTE: Additional Steps for Other Hard Drives

Hard drives from devices other than MobileView devices require an additional step as described in **step 3**. These devices also do not have the **Cameras** tab on the Properties window. Step 7 is therefore only applicable to MobileView devices.

To change hard drive properties:

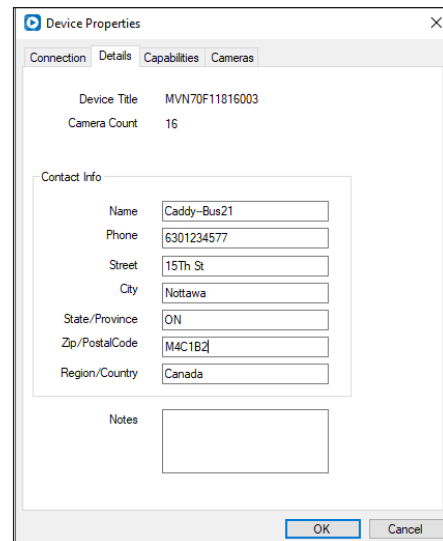
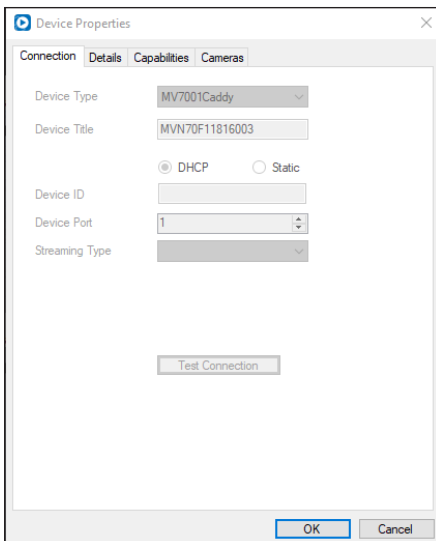
1. Log in to Evidence Manager.
2. Expand **Docking Stations** under **Home** , find a docking station.
3. Right-click this docking station, and click **Properties**. The **Properties** window appears.
4. Under **Connections**, view the connection details of the hard drive such as device ID, type of IP address, and device port.



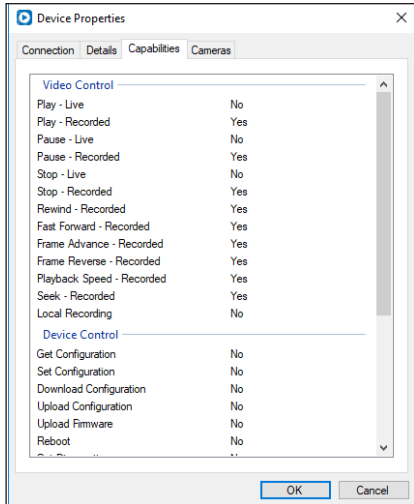
5. Under **Details**, do the following:
 - a. **Name:** Enter a name for the person who maintains the docking station.
 - b. **Phone:** Enter a phone number for this person.
 - c. **Street, City, State/Province, Zip/PostalCode, and Region/Country:** Use these fields to enter the maintenance personnel's address.
 - d. **Notes:** Notes, if any.

Note: Connection Details

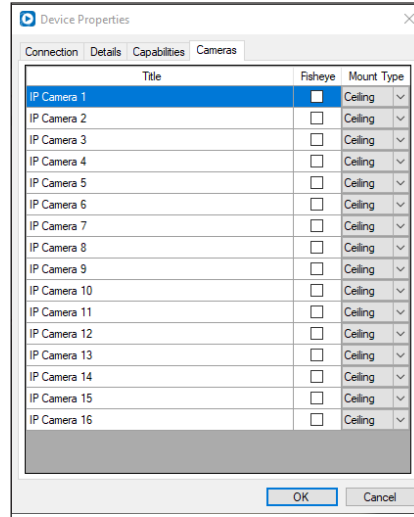
You cannot change the connection properties from here. To do this, see ["Adding a Device to the Devices Folder"](#) on page 23.



- Under **Capabilities**, view the following for this hard drive: Video Control, Device Control, Connection Types, and Other capabilities.



- (*MobileView devices only*) Under **Cameras**, view the camera details.
- Click **OK**.




Obtaining the HDD Log of a Docking Station

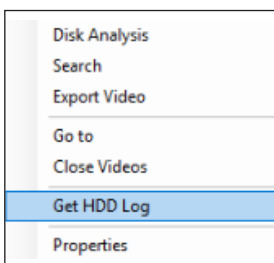
The HDD log is a log file of the hard drive of a docking station. It functions as a health report of the hard drive, which can be used to identify deviations from expected behavior.

NOTE: For What Devices Are HDD Logs Available?

At the moment, HDD logs are only available for MobileView devices.

To obtain the HDD log:

- Log in to Evidence Manager.
- Expand **Docking Stations** under **Home** , and find the docking station of your choice.
- Right-click this docking station, and click **Get HDD Log**.



The HDD log file is downloaded to your computer.

From a docking station, you can perform operations such as:

- Searching for videos using alarms and events
- Exporting videos
- Accessing disk analysis
- Searching for a video using the calendar
- Obtaining a HDD log
- Viewing docking stations properties

i NOTE: Searching and Exporting Media

The procedures for searching for and exporting videos are similar to the ones described in the topic **Managing Evidence**. The instructions can be found in the **Evidence Manager User Guide**.

Accessing Disk Analysis Data


Disk analysis is a color-coded graphical representation of the type of data that is stored on the hard drive within a docking station. It displays information such as total recorded video, alarms, events, video loss, and accelerometer data.

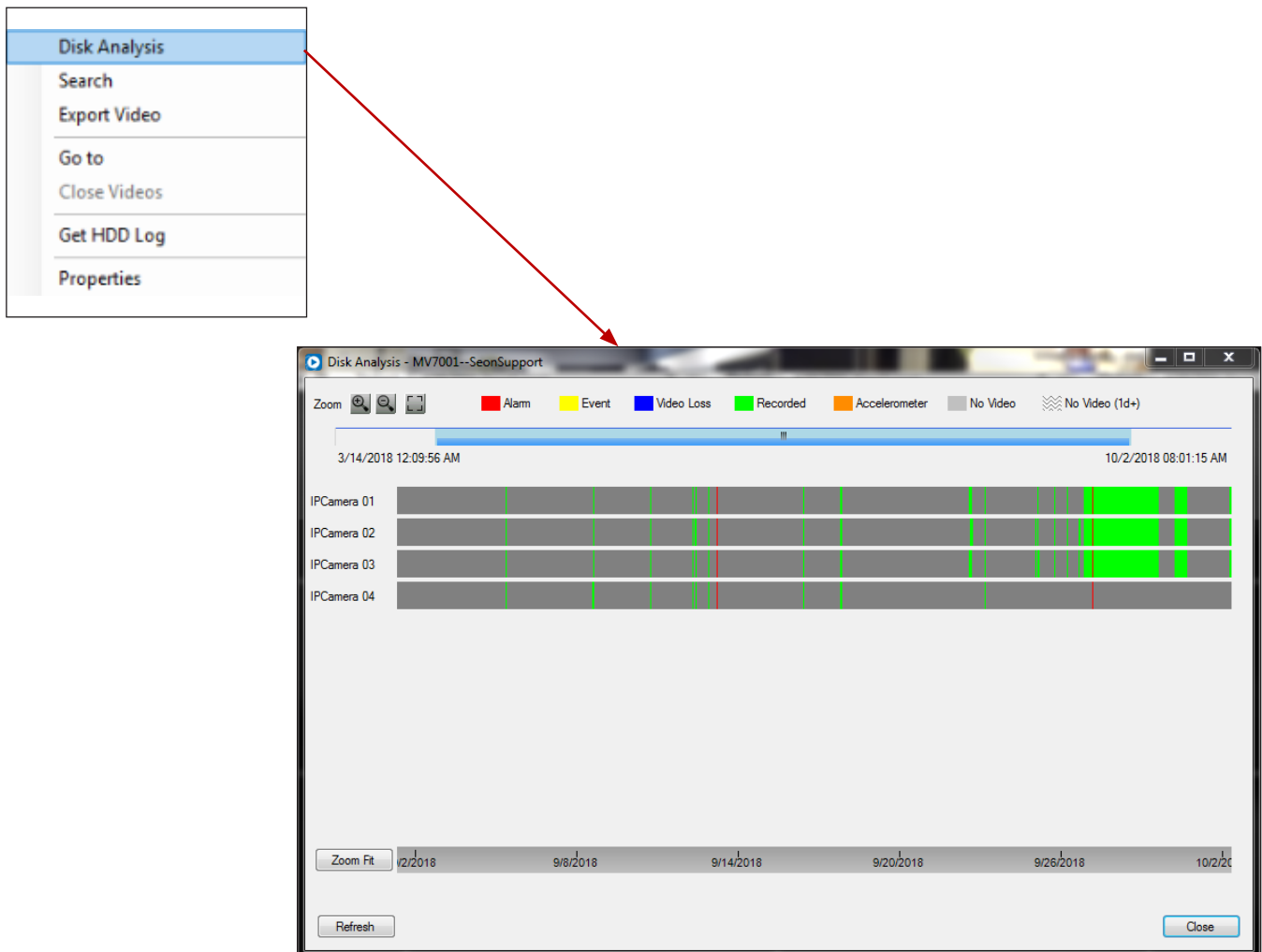
A docking station behaves similar to a device (recorder). That is why this procedure is exactly the same as the procedure described in the **Managing Devices** chapter.

i NOTE: Gray Periods on Disk Analysis

On a disk analysis display, periods where no video was recorded are displayed in gray.

To access disk analysis data:

1. Log in to Evidence Manager.
2. Expand **Docking Stations** under **Home**  in the left pane, and find the docking station of your choice.
3. Right-click this docking station, and click **Disk Analysis**. Evidence Manager retrieves and displays the disk analysis data in the **Disk Analysis** window.



Understanding Disk Analysis Information

Use the legend at the top to get a sense of the type of data that this device contains.

Zooming In/Out of the Disk Analysis Information

Use the zoom controls in the top-left corner for zoom-in, zoom-out, and zoom-fit controls.

OR

Click **Zoom Fit** in the bottom-left corner for zoom-fit controls.

OR

Use the scroll wheel of your mouse to zoom in or zoom out of the video.

Playing Video From this Hard Drive

Double-click the graph at the point that represents the start time of the video. Periods with no video are displayed in gray.

Viewing the Most Recent Disk Analysis Data

Click **Refresh**.

Support Information

Contact customer service

Technical Support: 1.844.899.7366

General Inquiries: 1.877.630.7366

Email: PTsupport@safefleet.net

Product information

For product information and related documentation, please visit the Safe Fleet Community:

<https://community.safefleet.net/>

Please contact Technical Support if you do not have credentials to log in.

Warranty

Complete warranty details are available at:

<https://community.safefleet.net/>