



Evidence Local User and Admin Guide

Rev: 04 Dec 2023

Axon Enterprise, Inc.
17800 N 85th St
Scottsdale, AZ 85255
USA

▲, ▲ AXON, Axon Dock, Axon Evidence, and Axon Fleet are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information, visit www.axon.com/legal.

All rights reserved. ©2023 Axon Enterprise, Inc..

App Store is a trademark of Apple, Inc. registered in the US and other countries. iOS is a trademark of Cisco Technology, Inc., Play Store and Android are trademarks of Google, Inc.

Microsoft, Windows, and Internet Explorer are trademarks of Microsoft Corporation registered in the US and other countries.

Contents

Overview	1
About this guide	1
Default account	1
Sign in	2
Main window	3
Search pane	5
Geo-fence	5
Set a geo-fence using coordinates	5
Set a geo-fence using the map	6
Create predefined geo-fence maps	6
Time and date	7
Filters	8
Assets pane	10
Search results display options	10
Operation buttons	10
Context-sensitive menu	11
Metadata	12
File properties	13
Play audio or video files	15
Playback control	15
Take a video snapshot	15
Add a marker to a file	16
Edit a marker	17
Other player functions	18
View an image file	20
Standard image viewer functions	20
Advanced image viewer functions	21
File operations	22
Verify file integrity	22
File verification failures	23
Export a file	24
Convert a file	26
Burn a file	28
Merge video files	29
Report on a file	31
Tag a file	31
Add tags to multiple files	33
Edit and remove tags	34

Quick menu	35
Web client	35
Import	35
Transfers	37
User device settings	39
Administration	41
Respond map	42
Location map information	42
Navigate the map	43
Real-time alerts	44
Recording list and user search	44
Device marker information	45
Livestreaming	45
Audit trail	46
Manage inventory	47
Overview	47
Find inventory information	47
Cameras	47
Set a camera name	47
Change camera assignment	48
Vehicles	49
Add a vehicle	49
Edit vehicle information	50
TASER, change assignment	50
Manage users	52
Overview	52
Add a user	52
Edit a user	54
Force a password change	54
Assign a user to a group	54
Set user rights	55
Inherit rights from a group	56
List of user rights	57
Manage groups	60
Overview	60
Add a group	60
Edit a group	61
Add a group from Active Directory	61
Assign users to a group	62
Set group rights	63

Manage folders	65
Overview	65
Add a folder	65
Edit a folder	66
Set folder access control	66
Remove folder access	67
Associate folders with cabinets	68
Folder properties Files tab	68
Manage cabinets	69
Overview	69
Add a cabinet	69
Edit a cabinet	70
Set cabinet access control	71
Remove cabinet access	72
Add folders to cabinets	72
Cabinet properties Files tab	72
Manage tags	73
Overview	73
Create a tag template	73
Edit a tag template	75
Manage associations	76
Overview	76
Association examples	77
Example A	77
Example B	77
Create an association	78
Manage storage locations	80
Overview	80
Add a storage location	81
Edit a storage location	82
Change storage location priority	82
Manage ingestion points	83
Overview	83
Add an ingestion point	84
Change priority	84
Manage destinations	86
Overview	86
Add a destination	87
Add an Evidence.com destination	87
Edit a destination	91

Reports	92
Overview	92
System report	92
Camera report	93
TASER report	94
Manage file extensions	95
Overview	95
Add a file extension	95
Edit a file extension	97
Manage device settings	98
Overview	98
Body-worn camera (BWC) settings	98
Change settings	98
Body camera setting descriptions	99
Axon View	102
Global settings	102
Fleet settings	102
Change settings	103
Fleet setting descriptions	104
Axon Signal settings	105
Set Signal triggers	106
Respond settings	106
TASER 7 settings	109
TASER 7 setting descriptions	109
Manage system settings	110
Overview	110
Standard system settings	110
Retention settings	110
Password settings	111
Miscellaneous settings	111
Interface configuration setting	111
Destination transfer settings	111
Feature settings	112
Schedule system settings	112
Legacy system settings	112

Overview

Axon Evidence Local is Axon's on-premises digital evidence management platform. Axon Evidence Local lets you securely store, manage, and share all your digital evidence, regardless of source, within your own secure network.

Axon Evidence Local is a robust end-to-end solution that lets you not only store data, but dictate access control at a granular level, create unique chain-of-custody reports with the most comprehensive audit trail on the market, and automate workflows for managing and sharing that data securely.

Because of the uniquely configurable nature of Axon Evidence Local, your agency will have total control over how to set up the system to work best for you. Officers and command staff can easily upload content from any other source of digital evidence, manage it simply with configurable metadata fields, retrieve it with an advanced search engine, automate access control, storage location, and retention with intelligent workflow features, and then collaborate effortlessly with other stakeholders using powerful sharing features.

Evidence Local uses client-server architecture. It supports the use of Windows Active Directory users and Evidence Local-created users for system access authentication. Its users authenticate against the Evidence Local Server whereas Active Directory users authenticate through a domain server on the network.

About this guide

This guide describes how to use Evidence Local to interact with files and information. The first half of this guide is for all users, while the second half consists of topics intended for Evidence Local administrators (these topics are introduced as being for admins). For admin-level information on configuring and managing Evidence Local, jump to the first admin topic, [Manage inventory](#) on page 47.

If you need additional assistance, contact technical support at support@axon.com, 1-800-978-2737, or 1-480-463-2170.

Default account

When you first install Axon Evidence Local, it creates a default administrator account. Use this account to define security settings, create custom roles and permissions, add users (user administrator, armorer, or other types of custom roles), assign devices, create folder structures, set retention policies, and configure several other administrative features for your Axon Evidence Local system.

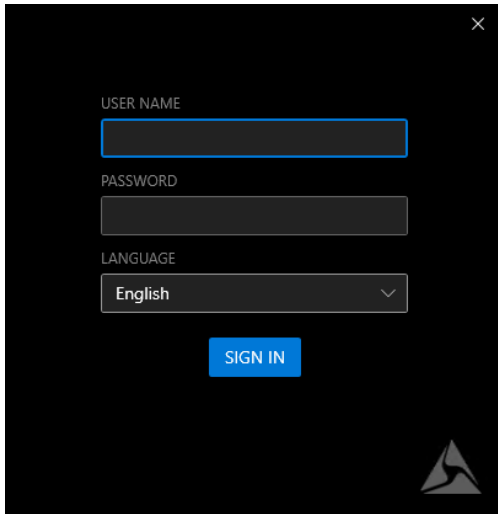
The default administrator account credentials are:

- **Username** – admin
- **Password** – pass

IMPORTANT After logging into Evidence Local as an administrator and creating your own user account, don't forget to change the default administrator account password.

Sign in

1. Launch Evidence Local from the shortcut icon on your desktop or from the Start menu. To open the web client in a browser (Chrome, Edge, or Firefox), enter your URL: `https://{domain}.commander.evidence.com`.
2. Enter your **User name** and **Password**.



3. Select the **Language** for this Axon Evidence Local Client session. In a browser, select language at the top right of the window.
4. Select **Sign In**.

The user name can be from a domain or manually created within Axon Evidence Local Administration. If two or more instances of the user name are found, the client will ask you to choose the preferred domain or no domain.

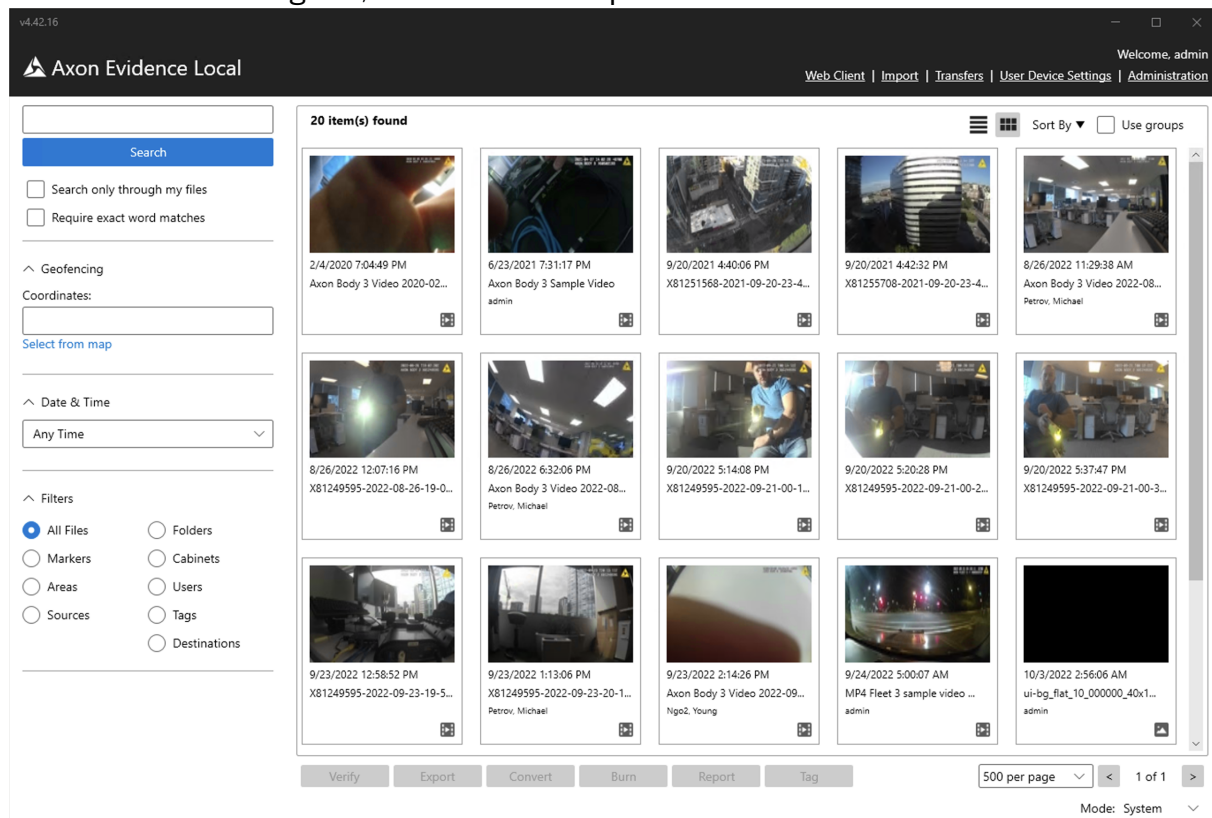
NOTE There's a link for Web Client link in the Quick menu on Evidence Local's main screen:

Welcome, Drew Smith
[Web Client](#) | [Import](#) | [Transfers](#) | [User Device Settings](#) | [Administration](#)

Evidence Local web client is the web-based version of Axon Evidence local client (computer app). They can be used simultaneously.

Main window

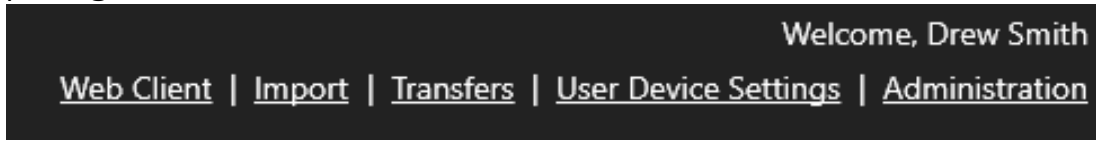
After a successful sign-in, Evidence Local opens to the main window.



The window is divided into three main sections: the upper right corner displays the welcome message with your name (below), the [Search pane](#) (page 5) is on the left side, and the [Assets pane](#) (page 10) is on the right.

The welcome message expands to show the Quick menu with **Import** (opens the Media Directory to import media files), **User Device Settings** (change settings for your

assigned devices), and **Administration** (administrative tasks). You may not have privileges to use all these functions.



Search pane

The Search pane on the left helps you find digital evidence files in Evidence Local.

Enter data in the box (such as name, address, title, or description) and select **Search** below it to search. To filter your results, use the criteria below the **Search** button.

- **Search only through my files** limits the search to only files you own.
- **Require exact word matches** limits the search to files that have an exact word match with the information entered in the search field.

Expand the **Geo-fence** (below), [Time and date](#) (page 1), and [Filters](#) (page 1) sections using the expand/collapse arrow at the left of each section.

Search results display in the [Assets](#) pane (page 10) grouped by date (default). Expand or collapse these groups like the Search pane sections. See [Search results display options](#) on page 10 for information on sorting and navigating the search results.

Geo-fence

Geo-fence lets you search for an asset file based on where it was recorded. This only works with files containing GPS information.

NOTE Axon Evidence Local Extractor extracts GPS information for video assets from Axon Body and Flex cameras paired with the Axon View mobile app. Location Tracking must be enabled in Axon View for the GPS feature to function correctly.

Enter map coordinates to define a search box or draw a search box on a map to search for asset files recorded within the search box.

Set a geo-fence using coordinates

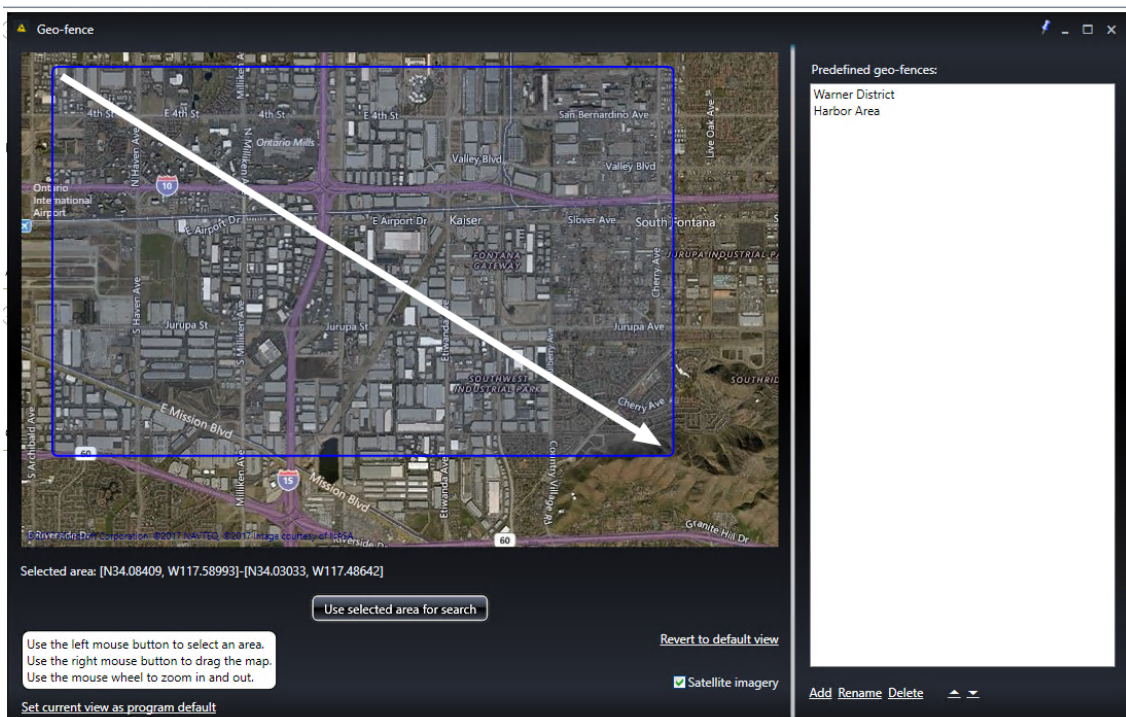
In the Geo-fence Coordinates field, enter, in brackets, the longitude and latitude coordinates (separated by a comma) for one corner of the search box. Enter a dash, then enter, in brackets, the longitude and latitude coordinates (separated by a comma) for the opposite corner of the search box. Enter coordinates in Decimal Degrees (DD) format.

Add the north, south, east, and west notations at the beginning of each coordinate.

Example: [N47.61, W122.35]-[N47.60, W122.31]

Set a geo-fence using the map

1. Select **Select from map** in the Geo-fence section of the Search pane.
2. Use your mouse to locate the area you want to use as a search box.
 - Hold the right mouse button to move the map.
 - Use the mouse scroll wheel to zoom in and out of the map.
3. Hold the left mouse button and drag the search area on the map. Click left again to clear the selection.

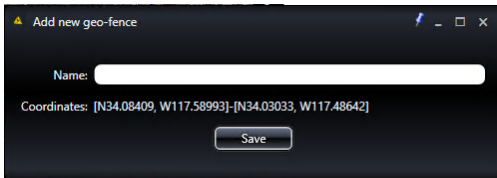


4. Select **Use selected area for search** to enter the map coordinates.

Create predefined geo-fence maps

If you use the same map areas during searches, save your geo-fence for next time.

Follow the same steps above, but after you've created the search box in step 3, select **Add** at the bottom of the right pane. Enter a name for the predefined map area and select **Save**.



Rename and **Delete** saved geo-fences as needed.

Time and date

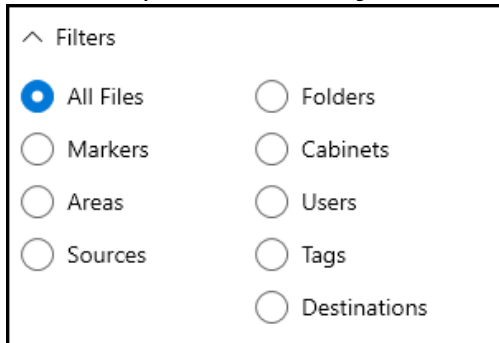
This section offers three methods of searching by time and date:

- **Any Time** searches through all files in the system, regardless of upload time.
- **Last *n* Days** searches through all files for that number of days in the past. This search is based on when the file was created, not when it was added to the system. The default value is **Last 30 days**. If you change the number of days, this becomes your new default value.

- **Range** searches through all files within the specified date and time.

Filters

Filters help narrow down your search results.



A screenshot of a 'Filters' menu. At the top is a chevron icon and the word 'Filters'. Below are nine radio button options arranged in two columns. The first option, 'All Files', is selected with a blue dot. The other options are 'Folders', 'Markers', 'Cabinets', 'Areas', 'Users', 'Sources', 'Tags', and 'Destinations'.

Filter Option	Status
All Files	Selected
Folders	Not Selected
Markers	Not Selected
Cabinets	Not Selected
Areas	Not Selected
Users	Not Selected
Sources	Not Selected
Tags	Not Selected
Destinations	Not Selected

When you select a filter other than **All Files**, a list displays below with options for that filter. You can only apply one filter and option at a time.

For many of these filters, use **Search for:** to narrow down a large list.

All files

Searches through all files. This is the default Filter selection.

Markers

Limits the search to files with the selected [marker](#) on page 16. Add markers to an asset as an Event Type. The list of possible Event Types is shown in the list box.

Use the **Search for:** field to narrow down the Event Types list by entering information into the field. This is useful if your system has many Event Types.

Example: To only show Event Types in the Assets pane with “traffic” in the title, enter *traffic* in the **Search for** field.

Areas

Limits the search to files from the selected area. The list of all available areas displays in the list box. These are typically areas that the files were created in or uploaded from.

Most systems have several areas that make sense for categorization within that specific solution.

Sources

Limits the search to files from the selected source. The list of available Sources displays in the list box.

The source usually pertains to the name of the system that generated or recorded the file.

Example: To search for assets from a particular camera, select the camera name in the list box.

Folders

Limits the search to files in the selected folder. The list of available folders displays in the list box.

Folders are for categorizing large groups of files. For admin-level details on folders, see [Manage folders](#) on page 65.

Cabinets

Limits the search to files in the selected cabinet, which is a parent directory to folders meant for a higher level of categorization of large groups of folders. For admin-level details on cabinets, see [Manage cabinets](#) on page 69.

Users

Limits the search to files associated with the selected user. For admin-level details on users, see [Manage users](#) on page 52.

Tags

Limits the search to files with the selected choice tags. Choice has a list of pre-defined values to apply to the file. Find information in text tags using the text Search field. For admin-level details on tags, see [Manage tags](#) on page 73.

Destinations

Limits the search to files that have been sent to another Evidence Local server or destination folder. Destinations are added to the system by Evidence Local administrators. Only visible as a search filter if they've been created and contain files. For admin-level details on destinations, see [Manage destinations](#) on page 86.

Servers

Limits the search to files associated with the selected server. Only visible as a search filter if another server has sent files to the Evidence Local server currently being accessed.

Assets pane

The Assets pane, on the right side of the main window, shows results from [searches](#) and lets you interact with digital evidence files.

Search results display options

The options at the top right of the Assets pane sets how your search results display:

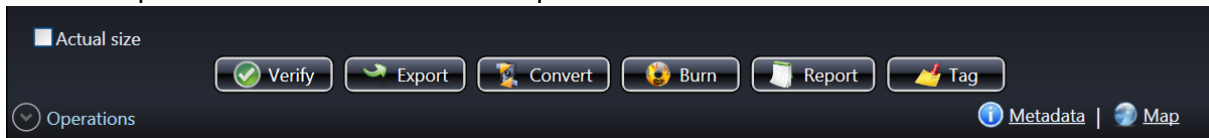


- The first two icons are for **List view**, which provides detailed file information, and **Gallery view**, which shows thumbnails and an abbreviated file information.
- **Sort By** sets the sort order of search results. There are several options for sorting results, including date and time, users, and file origin.
- **Use groups** will group search results by the selected **Sort By** option.

Navigation controls for the search results are at the bottom-left of the Assets pane. The bottom-right shows the total number of items in the search results.

Operation buttons

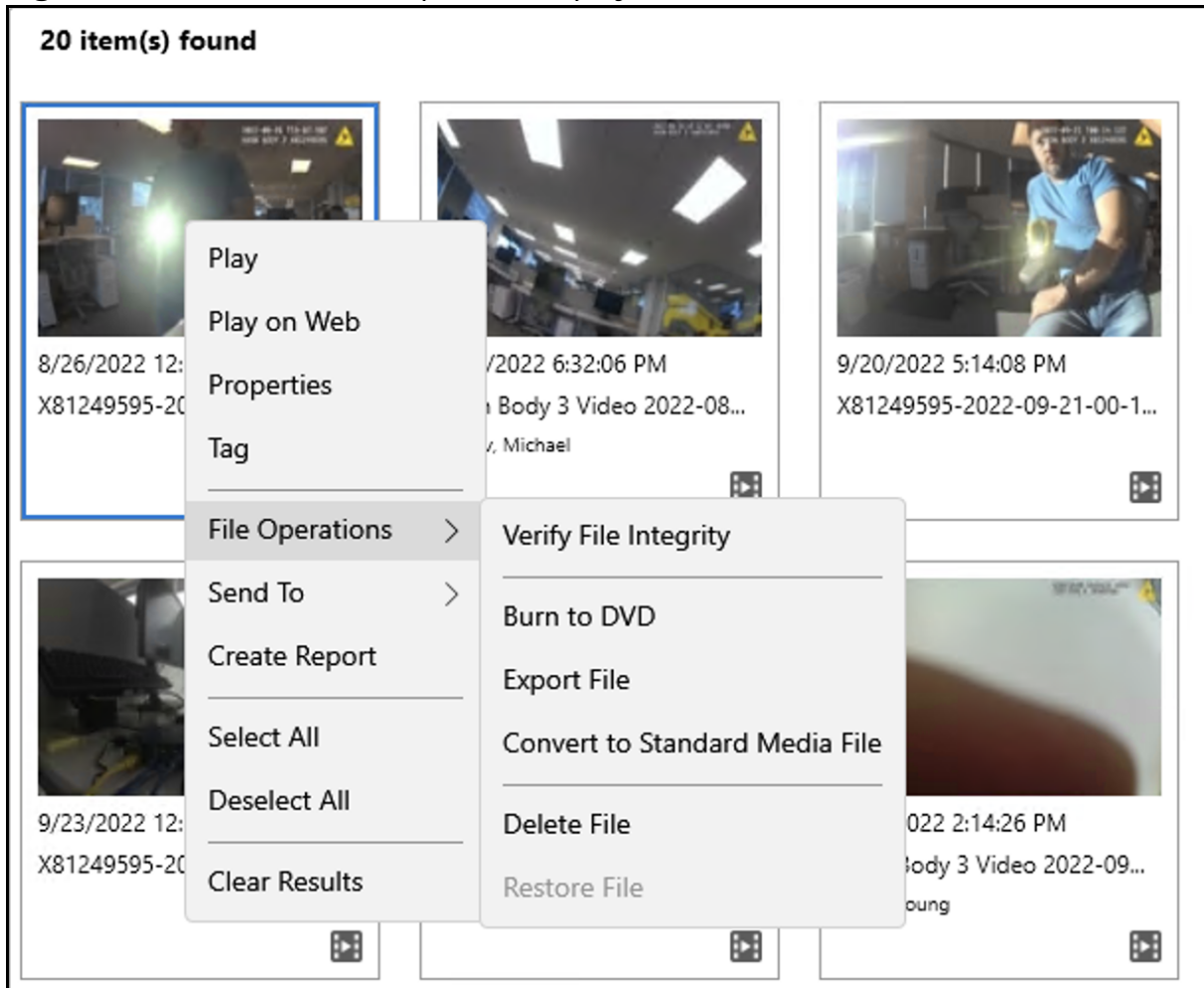
Use the operations buttons below the pane to interact with the selected files.



The six buttons shown above are only active when one or more files in the Assets pane are selected. For details, see [File operations](#).

Context-sensitive menu

Right-click a file in the Assets pane to display a context-sensitive menu:



Options include:

- **Play** – [Play audio or video files](#) on page 15
- **Play on Web** – Opens the evidence review page in a browser tab.
- **Properties** – Opens the Properties for the file (page 13)
- **Tag** – [Tag a file](#) (page 1)
- **File Operations:**
 - [Verify file integrity](#) (page 1)
 - [Burn a file](#) to DVD (page 28)
 - [Export a file](#) (page 1)
 - [Convert to Standard Media File](#) (page 24)

- **Delete File** – Moves the file to the recycle bin where it can be permanently deleted or restored to its original location.
- **Restore File** – Restores a file from the recycle bin folder to its last location.
- **Send To** – Sends the file to a predefined cabinet or folder. The cabinet or folder must first be created by an administrator, who must also set the option to allow files to be sent to it. See Adding a Cabinet or Adding a Folder.
- **Create Report** – Displays a report on all activity for the file. See Running a File Report.
- **View Metadata** – For image files, shows any Exchangeable image file format (Exif) information associated with the file, such as location and camera information.
- **Select All** – Select all files on the current Asset pane page.
- **Deselect All** – Cancels the selection of all files.
- **Clear Results** – Clears search results from the Assets pane.

Metadata

Each asset includes metadata information:

- **List view** shows a thumbnail preview of the file, the file title, file extension enter, user name, start date and time, duration, area, source, and server.
- **Gallery view** shows a thumbnail preview of the file, the start date and time, duration, file extension enter, and file title.
- Hovering over a thumbnail preview shows a pop-up with a thumbnail preview, title, start date and time, duration, owners, and extension.

NOTE Depending on how your system is configured, some files in the search results might be highlighted in red, indicating you do not have rights to access the files.

The different metadata fields include:

- **Thumbnail Preview** – This is a small image for video and image files.
- **Title** – The title given to the file.
- **User name** – The name of the user that owns the file. This is usually shown in the format Last Name, First Name. If the user's full name is not entered, the user's Login name is shown.
- **Owner/Second Owner** – The Username of the user that owns or is the second owner of the file.
- **Area** – The location given to the file.
- **Source** – The device that recorded or provided the file.
- **Start Time** – If the file is a video or audio file, this is the start date and time. Otherwise, this is the last modified date.

- **Duration** – If the file is a video or audio file, this is the length of the recording. Otherwise, it is blank.
- **Extension** – An abbreviation indicating the format of the file.
- **Server** – The name of the Evidence Local server the file was transferred from. In single-server installations this field is blank.

File properties

If assigned the proper rights, you can modify some file properties and view other information about the file. Only the file Title, Description, Primary User, Secondary User, access controls can be modified. To modify properties:

1. Right-click the file in the Assets pane and select **Properties**. The **Cabinets**, **Folders**, and **Destinations** tabs on the Properties dialog box show the file associations with those objects.

Asset Properties

AXON_Body_2_Video_2017-03-22_1516-b135c981e5

Information | Cabinets | Folders | Security | Destinations

Title: AXON_Body_2_Video_2017-03-22_1516-b135c981e5

Description:

Primary User: admin - 1: admin

Secondary User: (none)

Start Time: 2017/04/13 21:30:20

End Time: 2017/04/13 21:31:10

Ingested At: 2017/04/18 11:51:54

Area: (blank)

Source: (blank)

Camera:

Server: DAVE-PC

OK Close Apply

2. Edit the file Title, Description, Primary User, and/or Secondary User as needed.

3. To change access control to the file, select the **Security** tab, which lists user and group access control (Allowed and Restricted) rules for the folder. The list is blank if this is the first time you are assigning access control to a folder.
 - Use the three lists and two check boxes used to create an access control rule.
 - **Selection list** – Selects the specific user or group to which the access control applies. The users or groups shown in the selection list is determined by which option is selected in the User/Usergroup list (see below).
 - **User/Usergroup list** – Sets if the Selection list (see above) shows a list of **Users** or **Groups**.
 - **Allow/Restrict list** – This sets the type of access control. **Allow** selected user or group access to the folder or **Restrict** it.
 - **Inherits security settings from cabinets and folders placed into** – When selected, the access control settings from a parent Cabinet or folder are inherited and apply to the file. This is selected by default.
 - After setting access, select **Add** to add the access control rule.
4. Select **Apply** to save the file property changes.
5. Select **Close** to exit the Asset Properties dialog box.

Play audio or video files

One of the most basic functions of Evidence Local is to play stored audio and video files. To play a file:

1. Search for the file.
2. Double-click the file in the Asset pane results (or right-click > **Play**) to launch the player.



Playback control



Standard playback controls include Play, Pause, and Stop of the file. Drag the scrub bar handle to move quickly through the file.

Multiple video players can be open at the same time, which is useful for analyzing events that happened at the same time from different points of view.

Take a video snapshot

The snapshot tool saves a selected video frame as an image file.

1. Open the video file in the player and pause at the desired frame.
2. Select **Snapshot** .
3. Enter or select the location, name, and file format for the image, then **Save**. The default file name is the local date and time when the snapshot was taken.

Add a marker to a file

Use markers to indicate a significant event in a video or audio file so that it can be accessed quickly in the future. In addition to manually adding markers in Evidence Local, camera users can add markers while the camera is recording in the field by pressing the appropriate button on their Axon body camera. Markers added using the button press are marked with a Camera Marker Event Type and can be edited in the same manner as other markers.

1. Open the video or audio file in the player.
2. At the appropriate point in the file, pause and select **Markers** at the bottom. The Markers dialog opens on the left side of the player.



The list at the top of the dialog shows the markers for the current file. The new marker is highlighted and has a timestamp and an initially blank Event Type.

3. Select **Add** at the bottom of the Markers dialog.
4. Enter or select an **Event Type**. If it exists in the system, select it from the list. Maximum length is 100 characters; all content will be searchable.
5. Enter a **Description**. This is an open field for simple comments or more detailed information. Maximum length is 7000 characters; all content will be searchable.
6. **Save** the marker.
7. Repeat steps 2–5 to add more markers to the file.

Edit a marker

Markers added by pressing the appropriate button on an Axon body camera are tagged with a Camera Marker event type and can be selected and edited in the same manner as other markers.

1. Open the video or audio file in the player.
2. Select **Markers** at the bottom of the player. The list at the top of the dialog shows the current markers.



3. Select the marker and select **Edit**.
4. Set the **Event Type** and **Description** as needed.
5. **Save** your changes.
1. Open the video or audio file in the player.

2. Select **Markers** at the bottom of the player. The list at the top of the dialog shows the current markers.



3. Select the marker and select **Edit**.
4. Set the **Event Type** and **Description** as needed.
5. **Save** your changes.

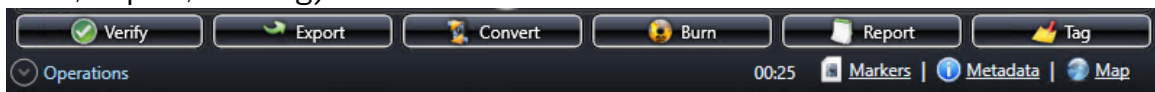
The marker is updated. You can search by the information contained in the marker.

Other player functions

- **Audio Mute** – Mutes the audio during playback. Some systems allow for the muting of left (CH1) and right (CH2) audio channels as shown in the image below. When video only supports one audio channel, only CH1 is available.

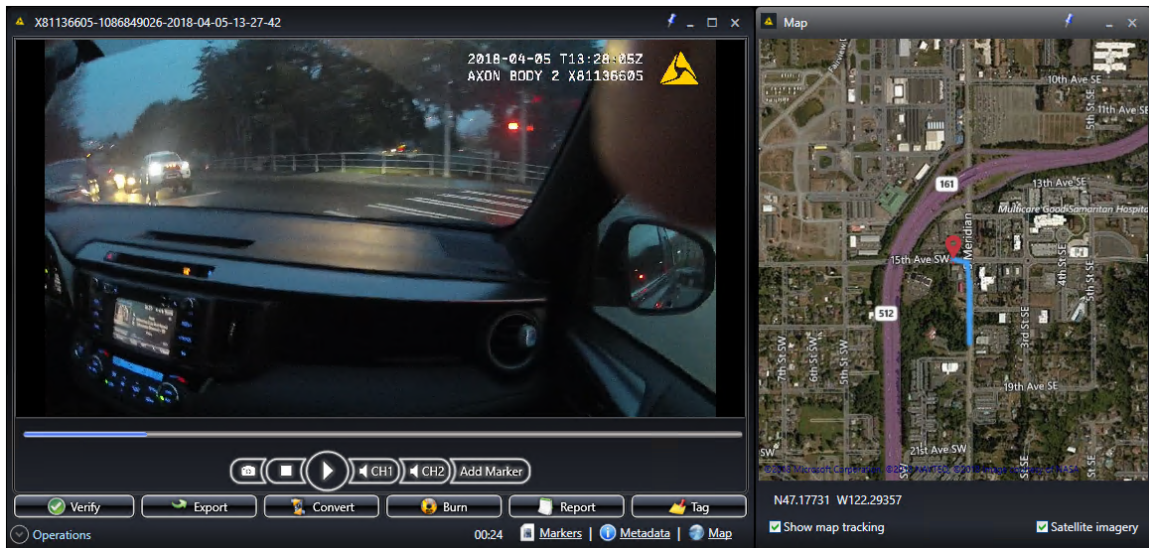


- **Operations** – Shows or hides the file operations buttons (Verify, Export, Convert, Burn, Report, and Tag).



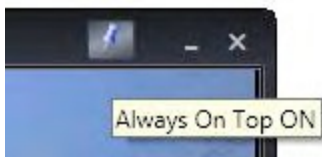
- **Map** – Opens the Map view and shows the GPS data associated with the video. If no GPS data is available, the map is blank.

When the Map view is open during video playback, the location shown on the map changes as the GPS position of the camera is updated. When viewing the map, hold the right mouse button and drag the map to change location shown. Use the mouse scroll wheel to zoom in and out of the map.



Use **Show map tracking** to add an overlay on the map that illustrates the route taken to get from one point to another.

- **Metadata** – Shows any GPS, radar, and triggers associated with the file. Also shows the last marker selected during viewing.
- **Markers** – Shows the Markers dialog. Double-clicking a marker jumps to the marker time in the file.
- **Always on top pin** – The pushpin control in the upper-right corner of the player keeps the player on top of all other windows, which is useful when viewing multiple players.

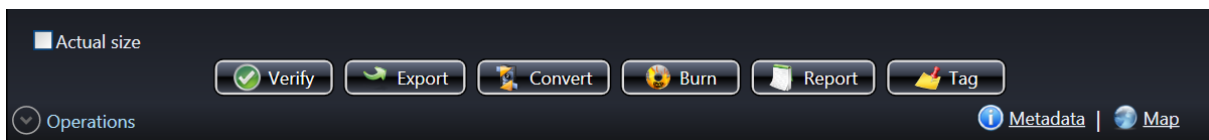


View an image file

Search for and select the file (double-click or right-click > Play) from the list in the Asset pane.



Standard image viewer functions



Actual Size – Select to show the image in its actual size. Otherwise, image are normally sized to fit the display window.

Metadata – Shows any Exchangeable image file format (Exif) information associated with the file, such as location and camera information.

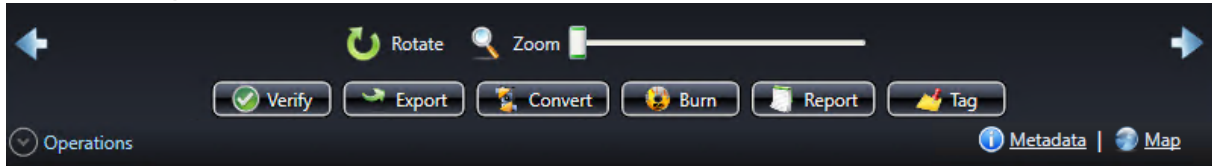
Map – Opens the Map view and shows the GPS data associated with the image file. If no GPS data is available, the view is blank.

Operations – Show or hide the file operations buttons (Verify, Export, Convert, Burn, Report, and Tag).

Always on top pin – The pushpin control in the upper-right corner of the player keeps the player on top of all other windows, which is useful when viewing multiple players.

Advanced image viewer functions

The Advanced Image Viewer must be enabled by your Evidence Local admin. It adds the following new functions:



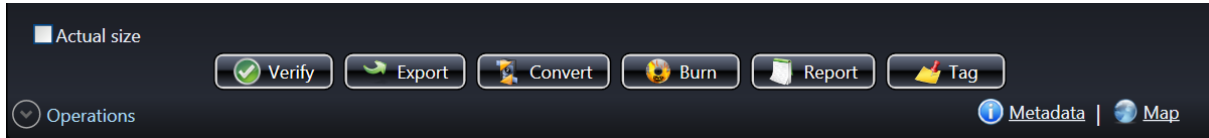
Rotate – Rotates the image file 90 degrees clockwise.

Zoom – Use this slider bar to zoom in or out of the image. When zoomed in, use your mouse to drag the image to view different areas.

Previous and **Next** arrows – These take you to the previous (left) or next (right) image in the Asset pane. If there are no previous or next images, that arrow is not shown.

File operations

The toolbar at the bottom of the viewer lets you perform the following functions on files in the Assets pane:



- Verify file integrity (below)
- [Export](#) a file (page 24)
- [Convert](#) a file (page 26)
- [Burn](#) a file (page 28)
- [Report](#) on a file (page 31)
- [Tag](#) a file (page 31)

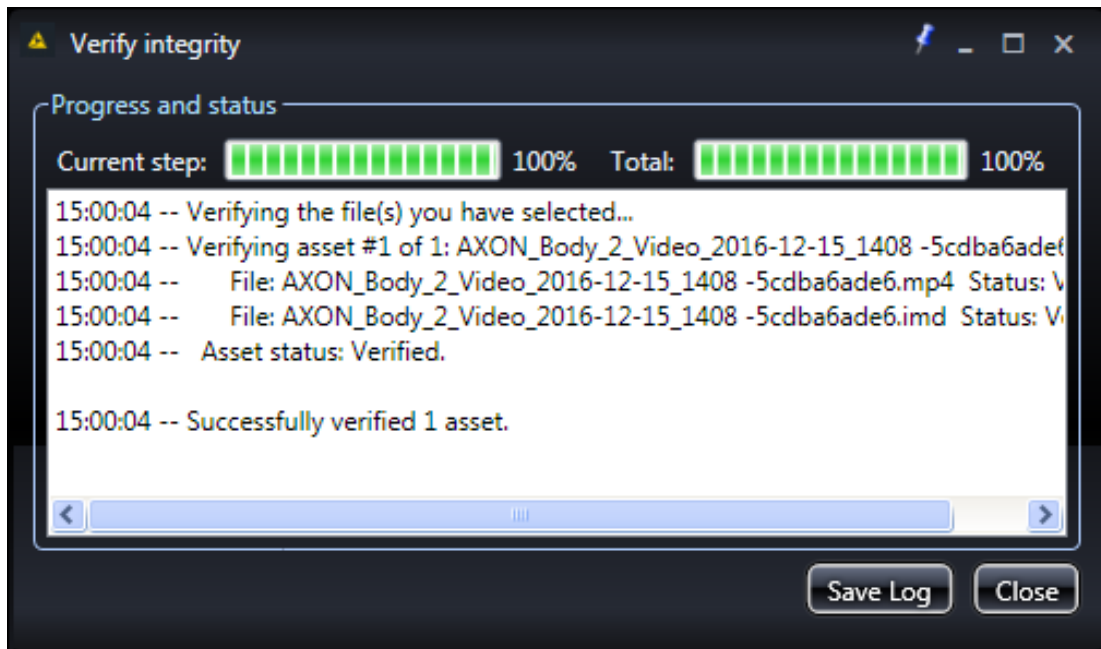
These functions are also available from the right-click [context-sensitive menu](#) on page 11.

Verify file integrity

All files ingested by Evidence Local are associated with an SHA-2 hash. This serves multiple purposes, the most important of which is to let Evidence Local identify and validate the files when they are moved due to association rules (admin-level details in [Manage associations](#) on page 76). The other purpose is to add a layer of security to prevent file tampering.

Users with appropriate permission can Verify a file to ensure it is whole and complete.

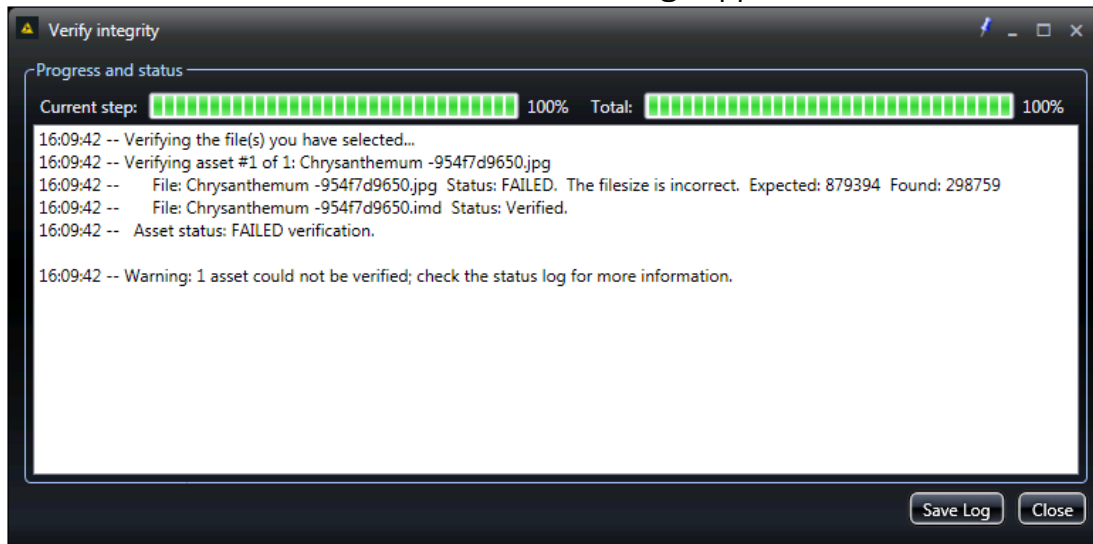
1. Select the file in the Assets pane and do one of the following:
 - Right-click and select **File Operations > Verify File Integrity**.
 - Select **Verify** at the bottom of the Assets pane.
 - Open the file in the player and select **Verify**.



2. Select **Save Log** if you want to save the process log.
3. Select **Close**.

File verification failures

If there is an issue with the File, a failure message appears:



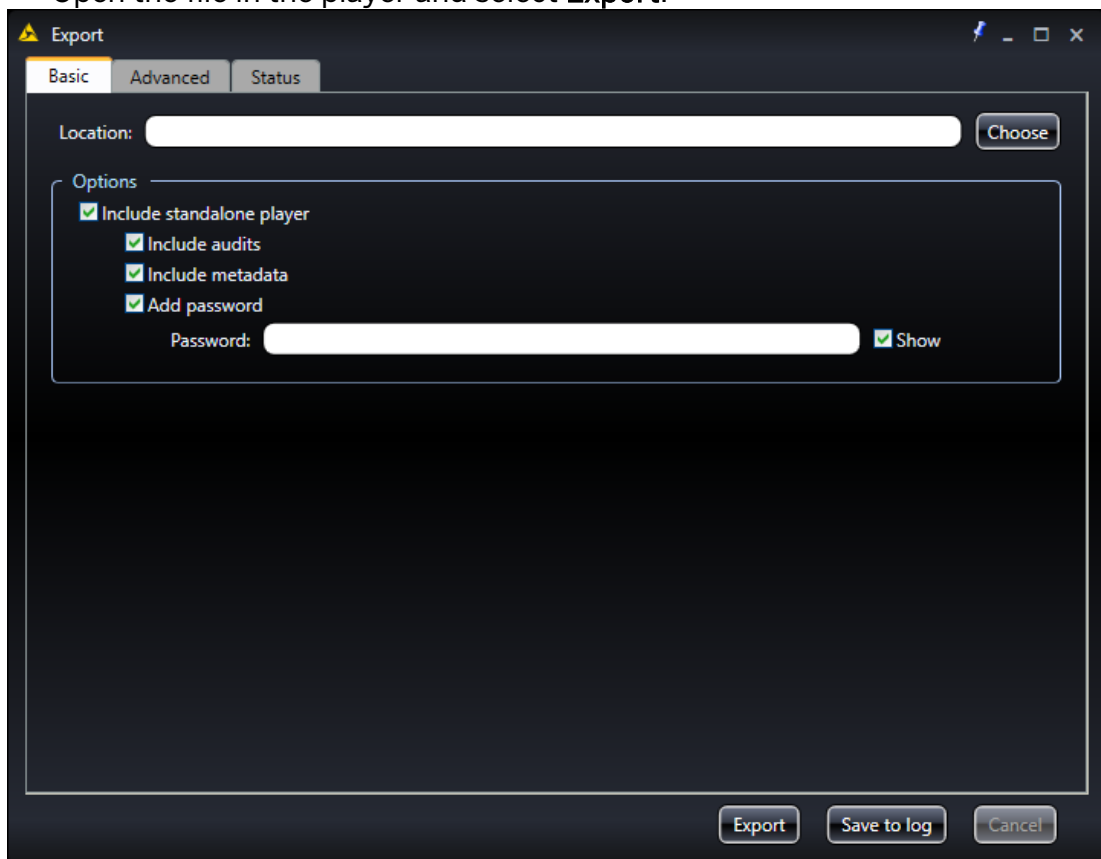
This example was verification of an image file that had a single pixel altered.

Export a file

A file in Axon Evidence Local can be exported for use externally. This is usually when some operation must be done with the file that is outside the scope of Evidence Local. Use Export to send a copy of the file to the requested location.

The export function allows you to export a selected portion (clip) of a file or several clips from the same file.

1. Select the file in the Assets pane and do one of the following:
 - Right-click and select **File Operations > Export File**.
 - Select **Export** at the bottom of the Assets pane.
 - Open the file in the player and select **Export**.



2. In the Export dialog box, select **Choose** to set the **Location** where the file will be exported.
3. Set export options as needed:
 - **Include standalone player** – Includes the Axon Evidence Local standalone media player in the export. The standalone media player allows a user to view the file and associated metadata outside of Evidence Local.
 - **Include audits** – Includes an encrypted file with a complete audit trail of the exported file.

- **Include Metadata** – Includes the metadata associated with the file in the export.
 - **Add password** – Requires a password before the file can be viewed in the Evidence Local standalone media player.
4. To specify a clip, select the **Advanced** tab. Otherwise, skip to the next step.

Export

Basic Advanced

Add asset:

#	Asset	Start point	End point	Action
1	AXON_Body_2_Video_2016-12-1	00:00:00	00:02:27	default

Starting point: Ending point: Action: ☒

Progress and status

File: 0% Total: 0%

- Select asset #1 in the list.
- Enter the time values for the **Starting point** and **Ending point** for the clip.

Starting point: Ending point: Action: ☒

- Select the appropriate **Action** (usually *default* or *Process*).
 - **Process:** Transcodes the file. If you are creating an authored DVD, it will make an MPEG 2 file (which DVD players support). Otherwise, it creates a WMV file.
 - **Direct Playback:** The file can be played directly within the standalone player. This information is included in the generated IPM file.

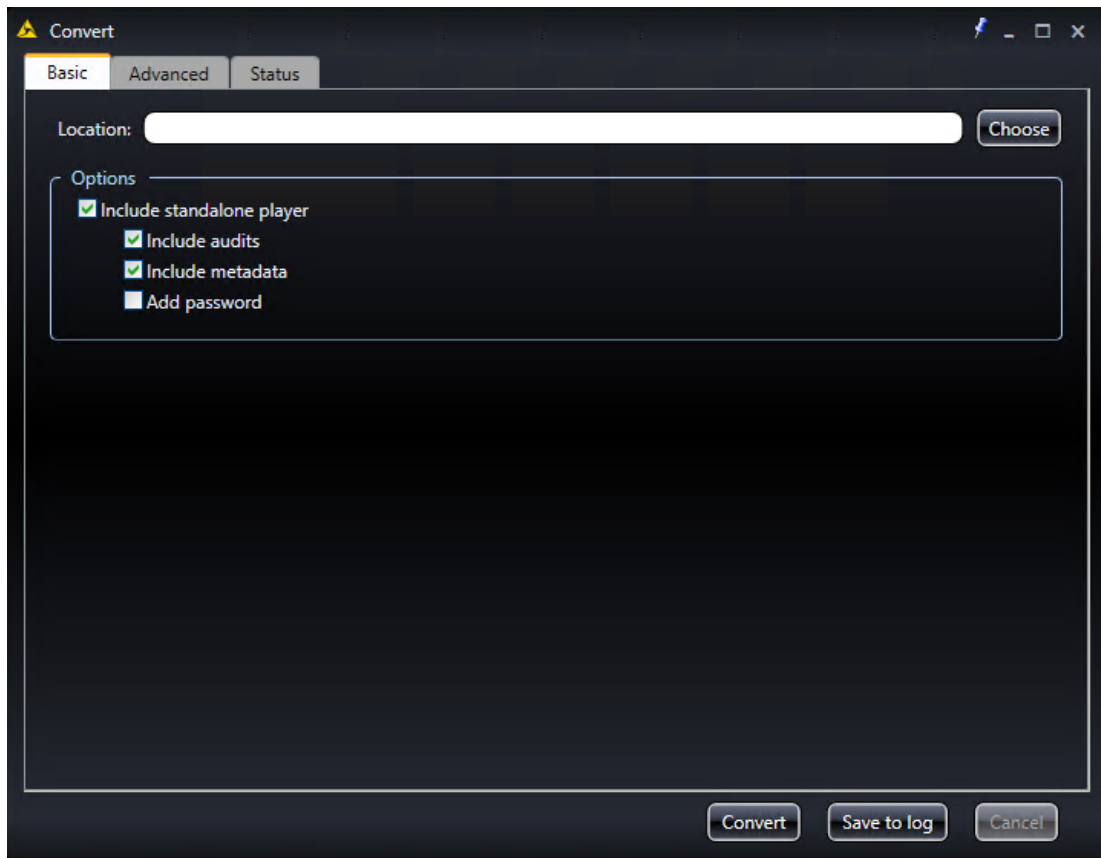
- **Export with IPM:** The file cannot be played directly within the standalone player. The generated IPM file includes information that tells the standalone player to inform viewers that the player can only show the metadata.
 - **Export without IPM:** Exports the file without an accompanying IPM file.
- d. **Save**  your changes.
 - e. To add another clip, select the file from the **Add asset** list and **Add asset to list** . Or, select an existing clip and **Duplicate selected clip** . Enter the time values for the **Starting point** and **Ending point** for the clip and **Save**.
 - f. To remove a clip, select the clip in the asset list and **Remove selected clip** .
5. Select **Export**. Status of the export displays at the bottom of the dialog box.
 6. If no longer needed, select **Cancel** to stop the process.
 7. After the export is completed, select **OK**.
 8. Optionally, select **Save Log** to save a text file of the export log.
 9. Close the Export dialog box.

Convert a file

If a file can be played with the Evidence Local player, it can be converted to WMV format and played with Windows Media Player. Evidence Local supports many types of files. However, some proprietary video files can only be viewed with an external player. These files cannot be converted by Evidence Local unless they are playable by DirectShow (a multimedia framework and API produced by Microsoft for software developers to perform various operations with media files or streams).

You can select multiple files for the conversion process, but only files that support conversion can be batch-converted.

1. Select the file in the Assets pane and do one of the following:
 - Right-click on the file and select **File Operations > Convert to Standard Media**.
 - Select **Convert** at the bottom of the Assets pane.
 - Open the file in the player and select **Convert**.



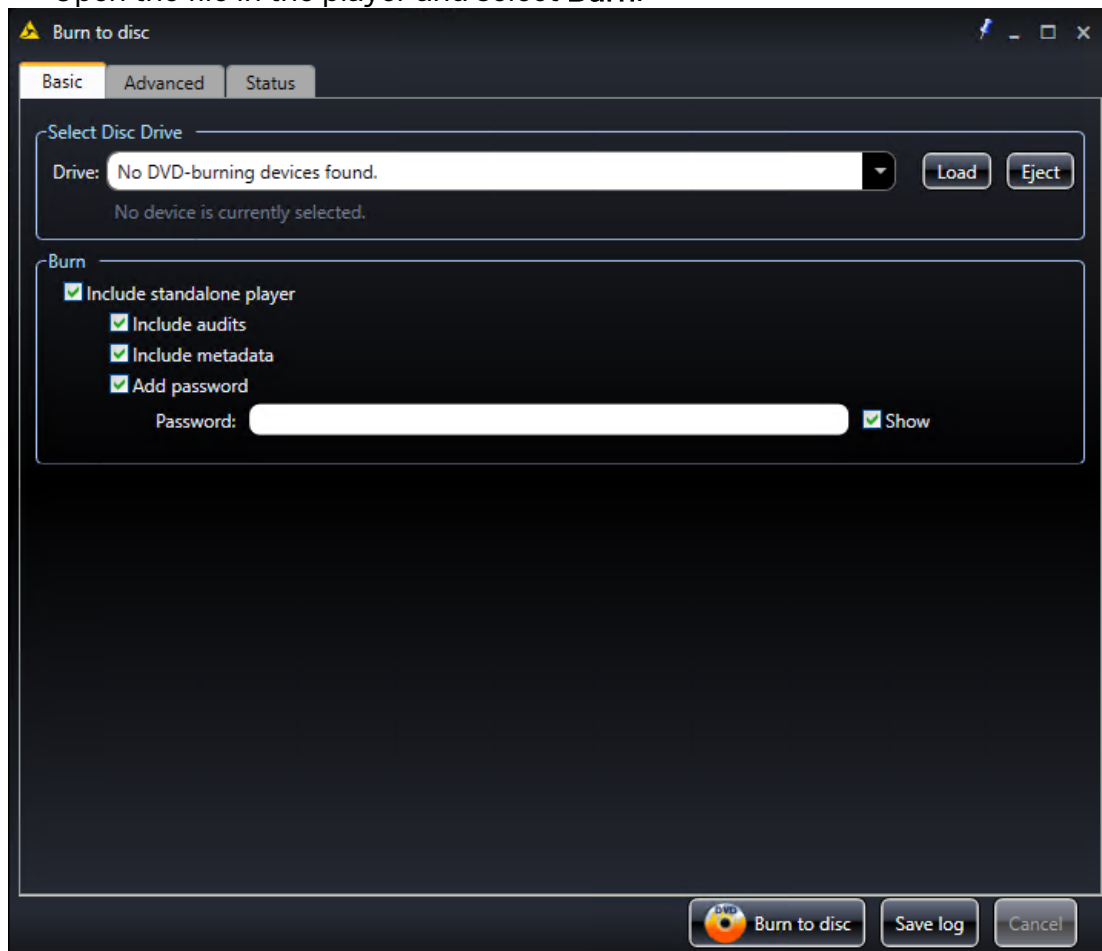
2. In the Convert dialog box, select **Choose** to set the **Location** where the converted file will be saved.
3. Set export options as needed:
 - **Include standalone player** – Includes the Evidence Local standalone media player in the export. This allows a user to view the file and associated metadata outside of the Evidence Local.
 - **Include audits** – Includes an encrypted file with a complete audit trail of the exported file.
 - **Include metadata** – Includes the metadata associated with the file in the export.
 - **Add password** – Requires a password before the file can be viewed in the Evidence Local standalone media player.
4. Select **Convert** to start the conversion. The time required depends on the size of the video file. The status of the conversion displays at the bottom of the dialog box. When the conversion process is completed, the WMV file is available at the location you specified.
5. If no longer needed, select **Cancel** to stop the process.
6. After the conversion is completed, select **OK**.
7. Optionally, select **Save Log** to save a text file of the conversion log.
8. **Close** the Convert dialog box.

Burn a file

You can burn files in Evidence Local to a data or authored DVD. Any files can be burned to a data DVD, but only video files that are playable in DirectShow can be burned to an authored DVD.

While you can burn multiple files to a data or authored DVD, the Authored DVD option is unavailable if any files contained in the selected batch cannot be burned to Authored DVD.

1. Select the file in the Assets pane and do one of the following:
 - Right-click on the file and select **File Operations > Burn to DVD**.
 - Select **Burn** at the bottom of the Assets pane.
 - Open the file in the player and select **Burn**.



2. In the Burn to disc dialog box, select the DVD Drive. Your DVD drive may be listed by default.
3. Ensure a disk is inserted in the drive.

4. Select Authored or Data:

- **Authored** – Authored DVDs can be played back in a standard DVD Player.
 - Only videos that support DirectShow Playback can be burned to an Authored DVD.
 - Authored DVDs do not display metadata during playback unless that metadata is overlaid on the video image itself.
 - The time needed to create an Authored DVD is proportional to the video length of the file plus additional time to finalize the DVD. This is because video Files need to be converted to a DVD readable MPEG2 format, placed in a .VOB container, and then burned to DVD.
- **Data** – Data DVDs contain the original files selected in the Assets pane. The Data DVD selection includes four options:
 - **Include standalone player** – Includes the Axon Evidence Local standalone media player on the DVD. The standalone media player allows a user to view the file and associated metadata outside of the Axon Evidence Local Client.
 - **Include audits** – Includes an encrypted file that has the complete audit history of the file.
 - **Include metadata** – Includes the metadata associated with the file.
 - **Add password** – Requires a password before the file can be viewed in the Evidence Local standalone media player.

5. Select **Burn to disc** to start the process.

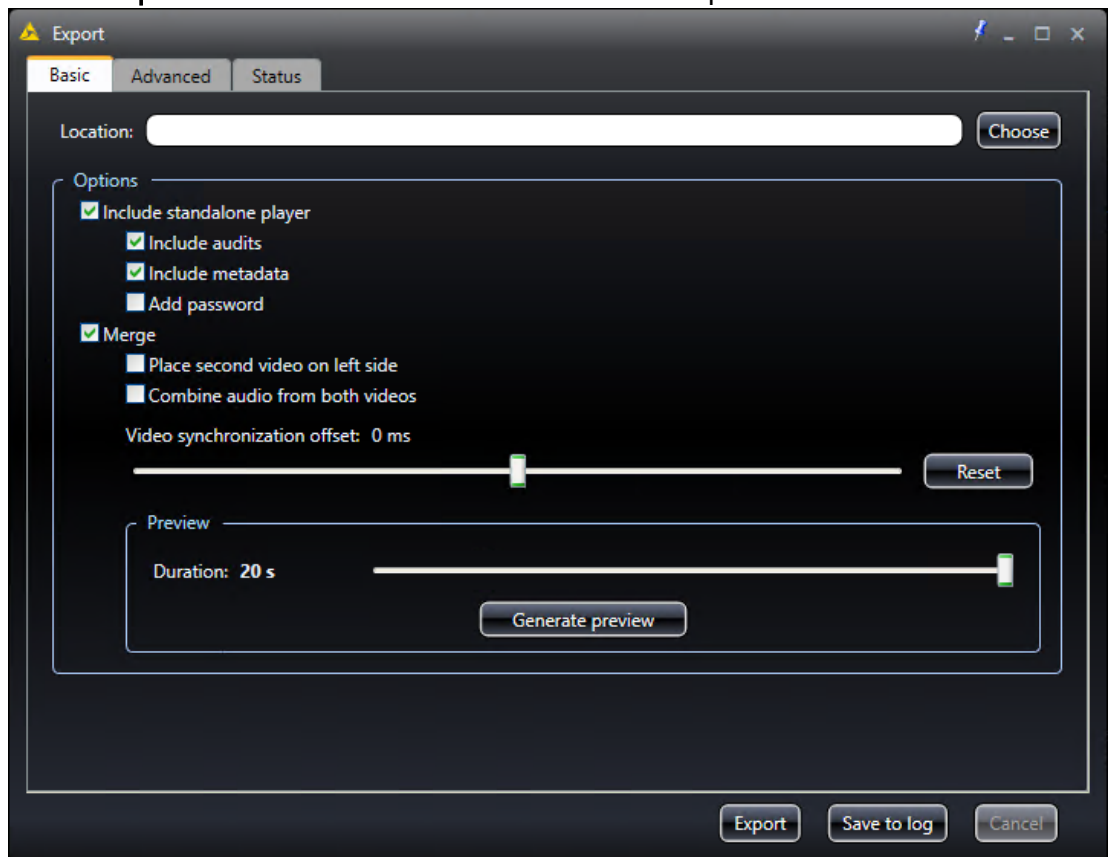
When the process is complete, the disc is ejected.

Merge video files

Evidence Local can merge two videos of the same file type when exporting or burning to DVD so they can be played back side-by-side and synchronized. This option is useful anytime two cameras are recording one situation, such as in Axon Interview.

1. Select the two files you want to merge from the Assets pane (select on one file and then Ctrl+click the second file) and do one of the following:

- Right-click and select **File Operations > Export a File or Burn to DVD**.
- Select **Export** or **Burn** at the bottom of the Assets pane.



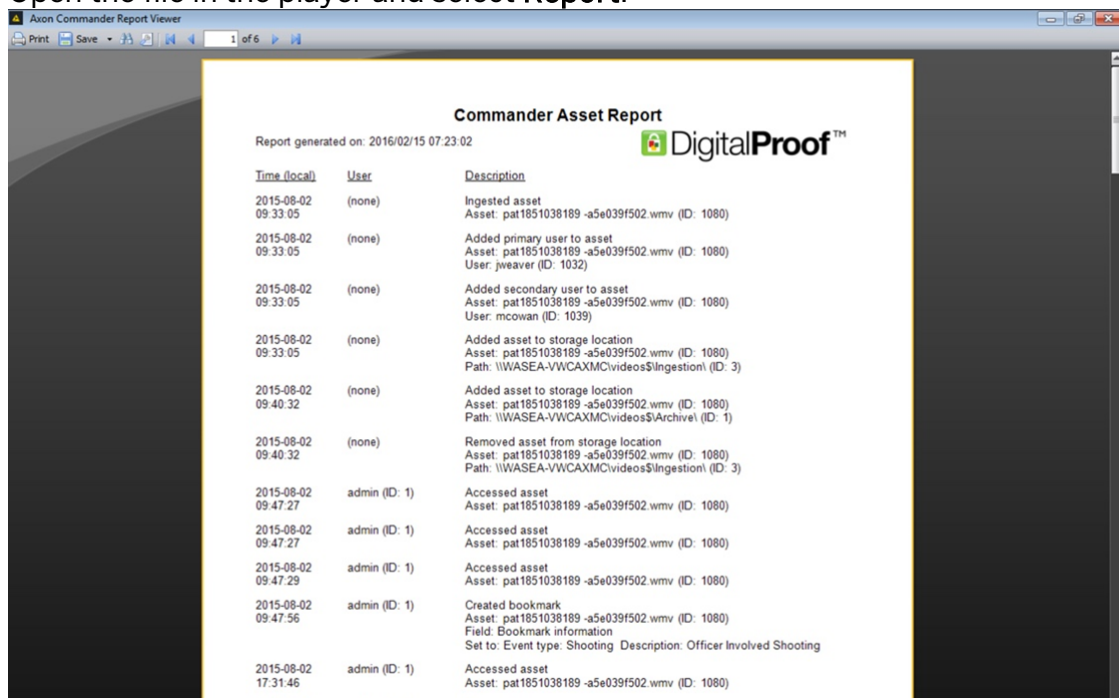
2. Select **Choose** to set the Location where the file will be exported or DVD drive.
3. Set export options as needed:
 - **Include standalone player** – Includes the Evidence Local standalone media player in the export. This allows a user to view the file and associated metadata outside of the Evidence Local.
 - **Include audits** – Includes an encrypted file with a complete audit trail of the exported file.
 - **Include metadata** – Includes the metadata associated with the file in the export.
 - **Add password** – Requires a password before the file can be viewed in the Evidence Local standalone media player.
4. Select **Merge**. Optionally:
 - Select **Place second video on left side**.
 - Select **Combine audio from both videos**.
 - Set the video synchronization offset for the two videos.
5. Select **Generate Preview** to review the merged video, audio, and synchronization.
6. If needed, adjust the merge settings.

7. Select **Export** or **Burn**. The status of the file operation displays in the Status tab.
8. If no longer needed, select **Cancel** to stop the process.
9. After the operation is completed, select **OK**.
10. Optionally, select **Save Log** to save a text file of the conversion log.
11. Close the dialog box.

Report on a file

A report lists an audit trail of actions performed on the file since it was ingested into Axon Evidence.

1. Select the file in the Assets pane and do one of the following:
 - Right-click on the file and select **Create Report**.
 - Select **Report** at the bottom of the Assets pane.
 - Open the file in the player and select **Report**.



In the report, entries where the user is listed as "(none)" indicate actions that were automatically completed by Evidence Local based on rules for the assignment and tagging of files.

2. Search, print, and/or save the report as needed.

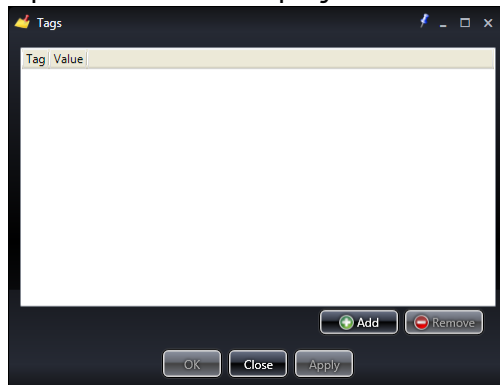
Tag a file

Any file in Evidence Local can be tagged. Tags are meta-information used to classify data for searching and for using Association rules.

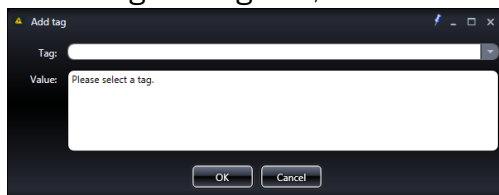
There are two types of tags: Text and Choice. Text tags apply free-form text to the file, while Choice tags have a list of pre-defined values to apply to the file.

After a tag is applied to a file, the tag information can be used when searching for files and invoking association rules (admin-level details in [Manage associations](#) on page 76).

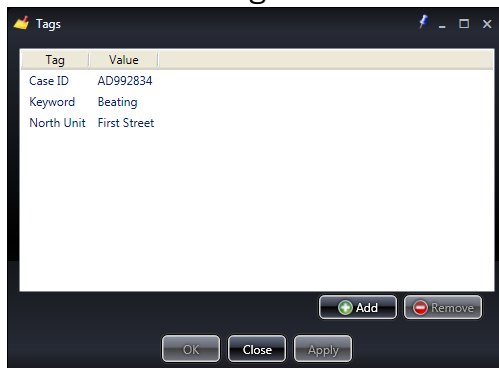
1. Select the file in the assets pane and do one of the following:
 - Right-click on the file and select **Tag**.
 - Select **Tag** at the bottom of the assets pane.
 - Open the file in the player and select **Tag**.



2. In the Tags dialog box, select **Add**.



3. Select a tag from the tag list.
4. In the **Value** box, enter or select the value for the tag.
 - For Text tags, enter the value.
 - For Choice tags, select the value.
5. Select **OK**. The tag name and value appear in the tags list.



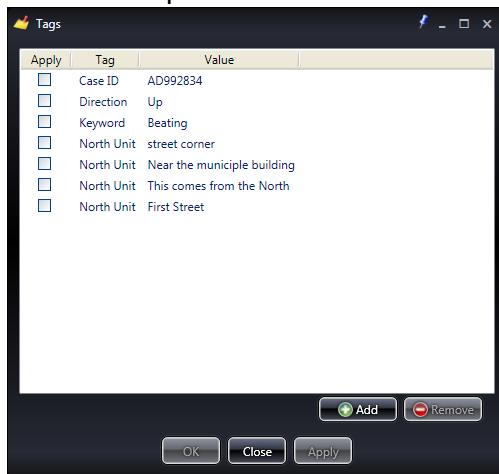
6. Repeat steps 2–5 to add another tag.
7. After all tags have been added, select **OK** to save the tags and return to the Assets pane.

Add tags to multiple files

To apply tags to multiple files at the same time:

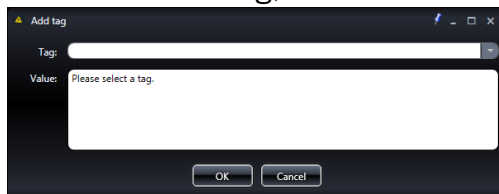
1. Hold the Ctrl key to select multiple files in the Assets pane.
2. Do one of the following:
 - Right-click and select **Tag**.
 - Select **Tag** at the bottom of the Assets pane.

When multiple files are selected in the Tags dialog box, an **Apply** column appears.



If the checkbox is selected for a tag, it's is applied to all selected files. If not selected, only one or some of the files have the tag applied to them. If the box is clear and then checked and you select **Apply**, all the files selected have that tag applied. Double-click a tag row to open the **Add tag** sub-dialog (shown in the next step) to modify the tag.

3. To add another tag, select **Add**.



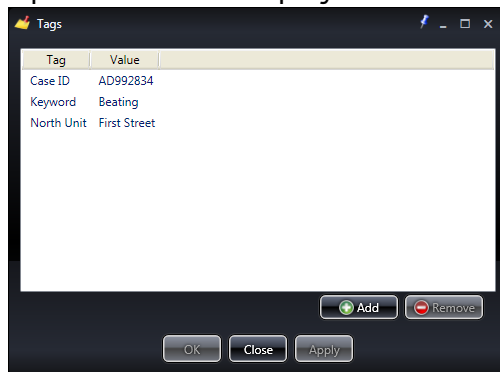
4. Select a tag from the **Tag** list.
5. In the **Value** box, enter or select the value for the tag.
 - For Text tags, enter the value.
 - For Choice tags, select the value.
6. Select **OK**. The tag name and value appear in the tags list.

7. Repeat steps 3–6 to add another tag.
8. After all tags have been added and selected, select **OK** to save the tags and return to the Assets pane.

Edit and remove tags

If allowed by the tag type, it can be edited or removed after being applied to a file.

1. Select the file in the Assets pane and do one of the following:
 - Right-click on the file and select **Tag**.
 - Select **Tag** at the bottom of the Assets pane.
 - Open the file in the player and select **Tag**.



2. To edit a tag value:
 - a. Double-click the tag name.
 - b. Enter or select the new tag **Value**.
 - c. Select **OK** to update the tag name and value in the tags list.
3. To remove a tag:
 - Select the tag name.
 - Select **Remove**.
 - Select **OK** to remove the tag from the tags list.
4. After all tags have been edited or removed, select **OK** to save the tags and return to the Assets pane.

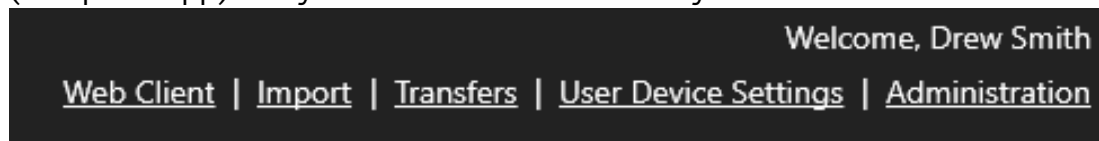
Quick menu

The Quick menu at the top right of the screen includes several important features of Evidence Local.

You may not see all of these features depending on your user permissions. Check with your administrator if you need additional permissions.

Web client

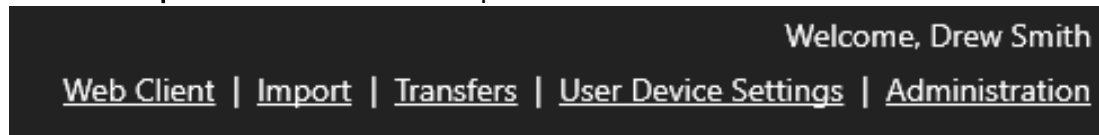
Evidence Local **Web Client** is the web-based version of Evidence Local client (computer app). They can be used simultaneously.



By default, Web Client opens to the [Respond map](#) on page 42.

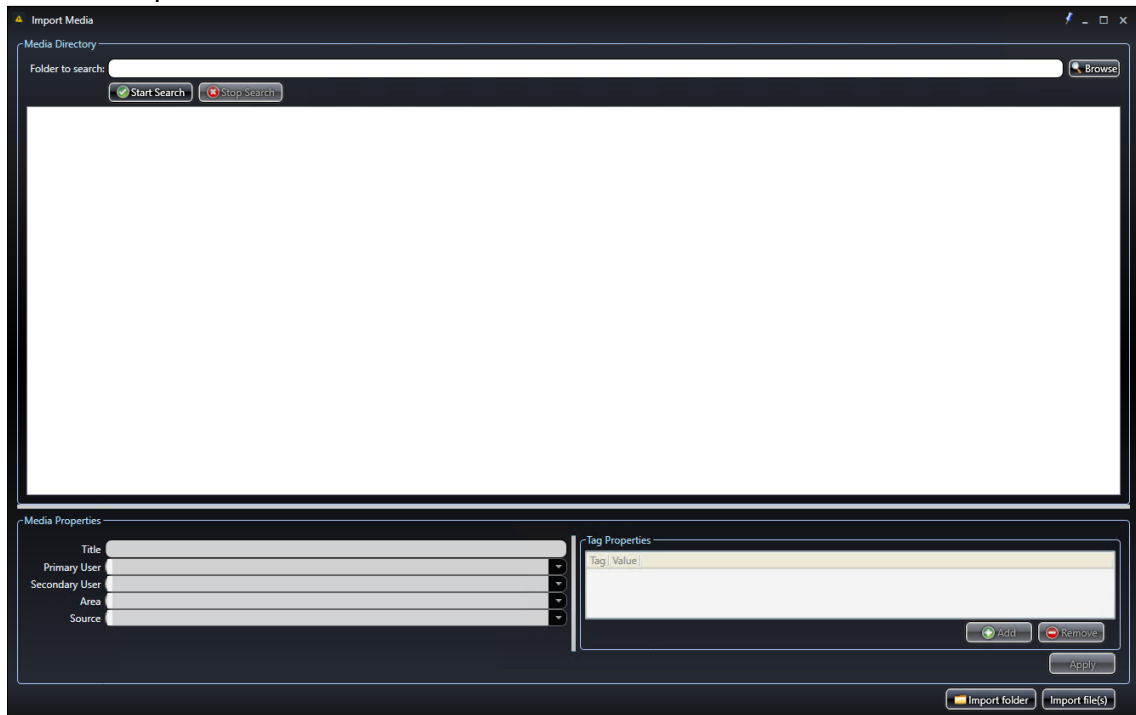
Import

Use the **Import** tool to find and import files into Evidence Local.



1. Select **Import** in the Quick menu.

2. In the Import Media window, either enter the path for the folder of the files you want to import or select **Browse** to find it.

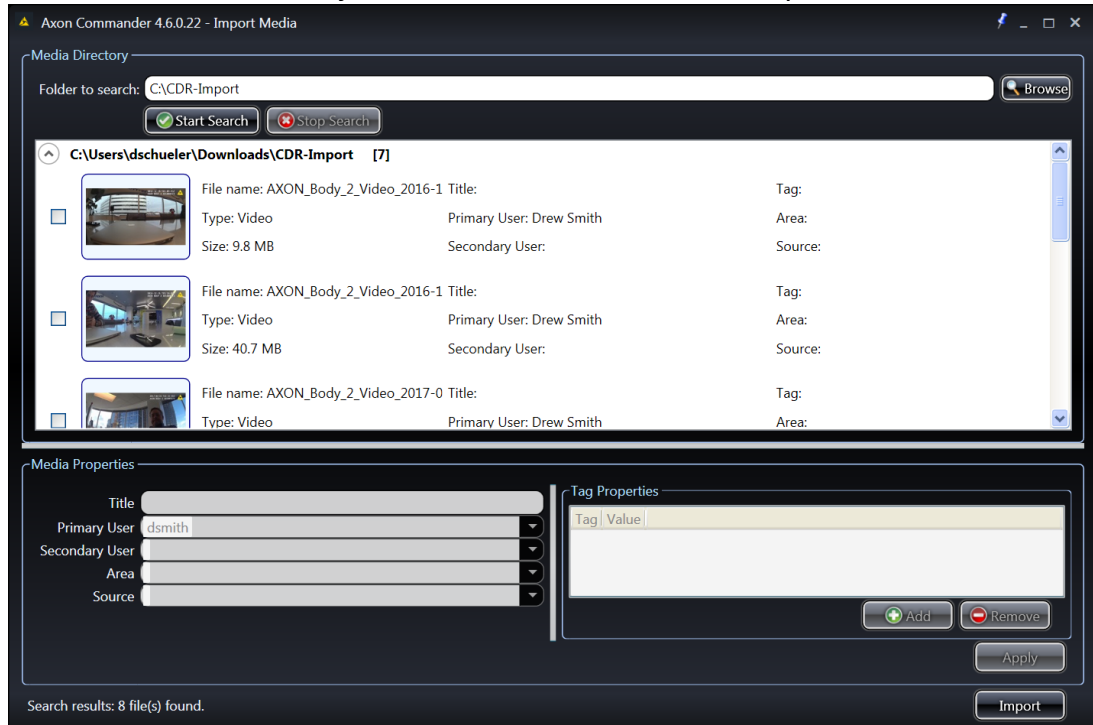


3. Select **Start Search** to begin looking for files. The search includes subfolders. It only searches for files with the extensions defined within the Extension Matrix that are enabled for import. All eligible files display in the window.

NOTE Every file loaded into the list consumes memory on your computer. If importing more than 100 files, use the Ingestion Point feature (admin-level details in [Manage ingestion points](#) on page 83).

4. To maintain the file structure of a folder when importing files from systems that need to maintain file structure, such as proprietary video systems or crime scene scanners, select the appropriate folder and then **Import Folder**. This creates a zip file with the folder contents to import.
5. To apply additional information to files for easier use in Evidence Local, select the desired files (or right-click for selection options like *Select all*), then:
 - Add additional data, including Title, Primary User, Secondary User, Area, and Source in the Media Properties section. After adding the information, select **Apply** to save the information.
 - Add tags in the Tag Properties section. Select **Add**, select the **Tag**, enter or select the Value, then select **OK**. Repeat to add more tags. Select **Apply** to save the information.

- Select the check box adjacent to the files to mark for import.

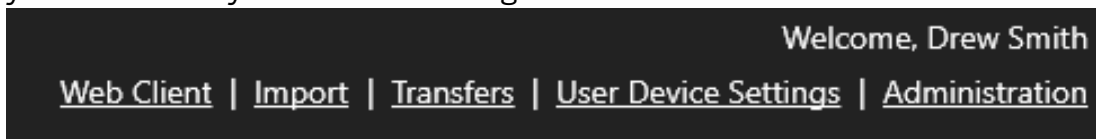


6. When finished selecting and preparing the files, select **Import**.

Imported files are processed by the system, so it may take some time for the files to be available for search and management by Evidence Local.

Transfers

Transfers lets you view inbound and outbound transfers for the Evidence Local server you are currently connected to using the Destinations feature.



Transfers are only available if you've been assigned the Manage Associations and Destinations right.

To view transfers, select **Transfers** from the Quick menu.

In the Transfers dialog box, each transfer in the queue will have one of the following status messages associated with it:

- **In-Progress** – A transfer is actively occurring, indicated by a percentage of transfer completion, the total, and the completed transfer size.

- **Pending** – An outbound transfer where the destination location is busy and unable to initiate a transfer. Transfers will leave this state when the destination server accepts the transfer.
- **Queued** – Transfer request is in the queue but has not started due to the number of simultaneous inbound or outbound transfers already being at maximum. Queued transfers will change to In-Progress after other transfers complete.
- **Waiting** – Transfer is unable to progress, typically due to connectivity issues. Transfers in this state will attempt to retry every 10 minutes.
- **Failed** – Transfer not possible due to an indeterminate issue. If transfers do not leave this state on their own, contact Axon Support for assistance.
- **Completed** – Transfer was successful and will be cleared from the queue in five seconds.

The screenshot shows a window titled 'Transfers' with a close button (X) in the top right corner. It is divided into two main sections: 'Incoming Transfers' and 'Outgoing Transfers'.

Incoming Transfers: This section has a table with three columns: 'File', 'Server (From)', and 'Progress'. The table is currently empty.

Outgoing Transfers: This section has a table with three columns: 'File', 'Server (To)', and 'Progress'. There is a 'Change Order' button with a double arrow icon in the top right corner of this section. The table contains four rows of data:

File	Server (To)	Progress
X81254464-2018-08-16-16-49-56 (1086849032).mp4	VM Server	2 MB / 8 MB (30%)
X81254464-2018-08-16-16-50-03 (1086849033).mp4	VM Server	4 MB / 8 MB (47%)
X81254464-2018-08-16-16-49-43 (1086849030).mp4	VM Server	Queued (8 MB)
X81254464-2018-08-16-16-49-49 (1086849031).mp4	VM Server	Queued (8 MB)

On the right side of the 'Outgoing Transfers' table, there are two circular arrows (up and down) for changing the order of the transfers.

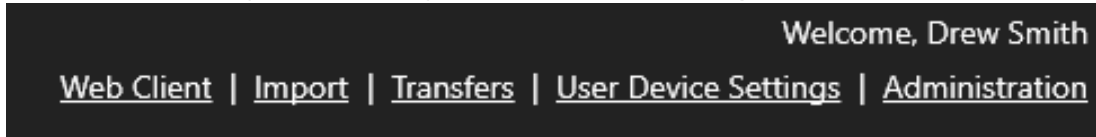
Modify the priority of outgoing transfers as follows:

1. Select **Change Order**.
2. Select on the asset you to modify and use the Up and Down arrows to change the priority.

You can't modify the priority of inbound transfers.

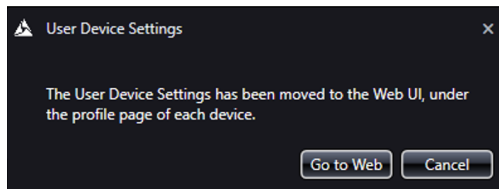
User device settings

This option lets you adjust settings for Axon cameras assigned to you within a web interface. It is only available if you have a device assigned.

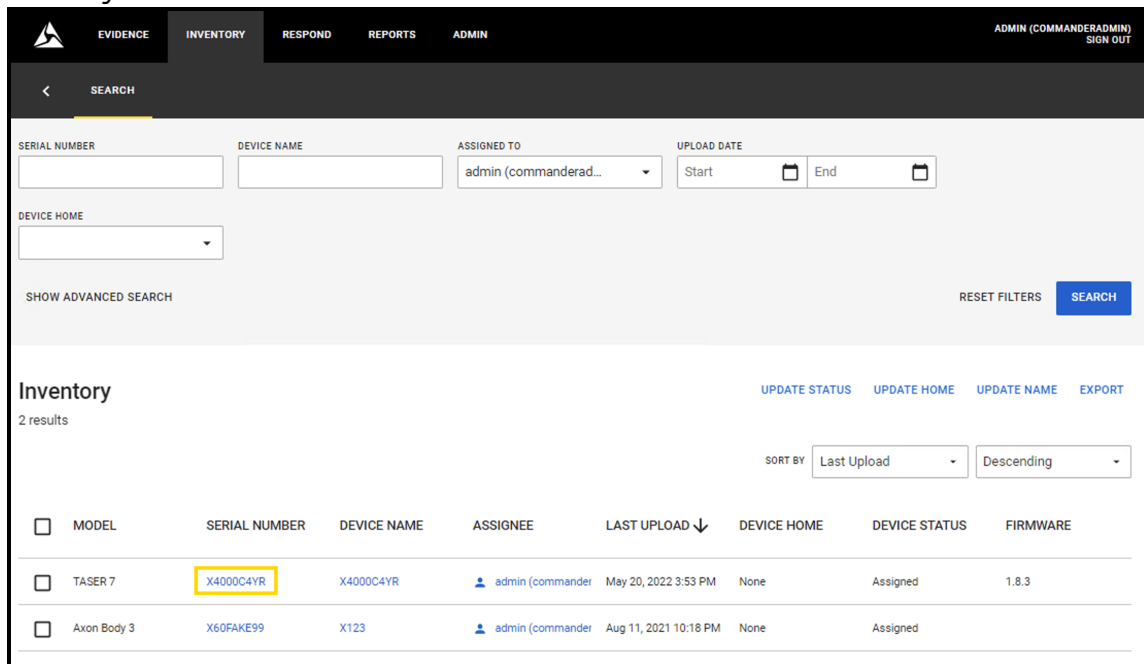


To modify device settings:

1. Select **User Device Settings**.
2. Select **Go to Web** to open the Evidence.com **Inventory** page on the default browser.



3. Select your camera serial number.



4. Adjust settings as needed. Settings you do not have access to or are inapplicable for the selected camera will be grayed out:

Device Settings

Speaker Volume

Controls volume of camera audio prompts.

☐ Highest

☐ High

☒ Medium

☐ Low

☐ Lowest

☐ Off

Vibration

Controls whether the camera uses vibration (haptic feedback) for camera notifications. Stealth must be disabled for this setting to be enabled.

☒

Indicator Lights

Controls whether the camera front and top LEDs emit light during operations. Stealth must be disabled for this setting to be enabled.

☒

Automatic Brightness

This mode automatically adjusts the brightness of front and top lights based on ambient light. If front lights are disabled, it only applies to top light. Stealth must be disabled for this setting to be enabled.

☐

Stealth

Controls whether the camera emits light, sound, and vibrations (haptic feedback) during operations.

☐

Available settings:

- **Orientation** – For Axon Flex 2 and Axon Flex cameras. The sets whether the camera is mounted on the right or left side of the user's body.
- **Speaker Volume** – Controls how loudly the camera beeps to communicate operations to the camera user.

- **Vibration** – Controls whether the camera uses vibrations to communicate operations to the camera user.
 - **Indicator Lights** – Controls the visible indication of the recording status on the front of the camera using the Triad LED. The light will blink green during pre-event buffering and red while recording. Disable Stealth mode to enable this setting.
 - **Automatic Brightness** – Axon Body 3 only. Enables Automatic Brightness mode to automatically adjust the brightness of front and top lights based on ambient light. If front lights are disabled, it only applies to the top light. Disable Stealth mode to enable this setting.
 - **Stealth Mode** – Controls whether the body camera emits light, sound, and haptic feedback (vibrations) when it is switched on or off and when you start or stop recording. In Stealth mode, all lights, sounds and vibrations are turned off; this will also disable Ring LED Status regardless of the Indicator Lights setting.
5. Select **Save Settings** to save the device settings.

Administration

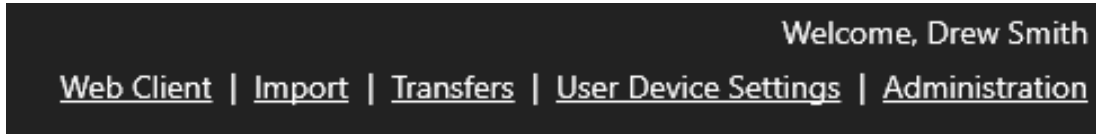
This feature opens administration-focused settings in Evidence.com. To start at the beginning of the admin topics, see [Manage inventory](#) on page 47.

Respond map

The Axon Respond map lets you see the location of Axon body cameras in a web browser. Viewing the map requires the **Respond view location map** permission.

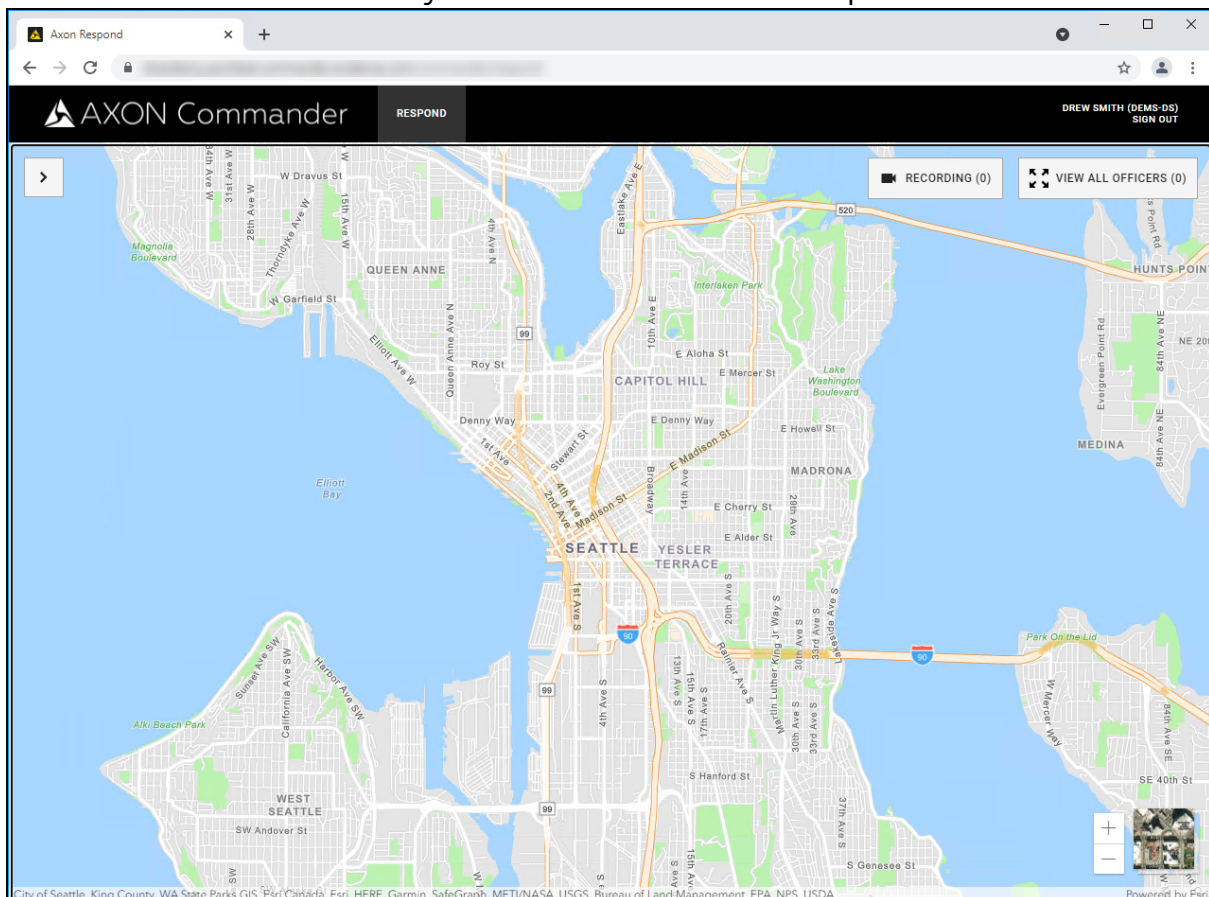
Axon Respond web only supports Google Chrome, Mozilla Firefox, Chromium Edge, and Safari desktop browsers. Internet Explorer and non-Chromium Edge are not supported.

To open the map, select **Web Client**.



Location map information

While recording, Axon body cameras send location updates based on the GPS sensor in the camera. Location updates are sent every few seconds while recording and stop when the camera stops recording. The Respond map and user list update with location markers based on when a body camera last sent a location update.



Icons on the map may include the following:

The center icon shows the camera type; this one is Axon Body 3. The color dot in the lower-right indicates the device status:

- A red dot ● means the device is recording.
- A green dot ● means the device is buffering. It may indicate the last reported location of the device location, depending on the device and agency settings.
- A gray dot ● means the device is off or docked. It may indicate the last reported location, depending on agency settings. The length of time it remains on the map depends on the Respond Device Location Filter setting for your agency.

A number marker indicates a cluster of multiple devices near the location. Zoom in to see individual camera markers. If devices are in different states, the color dot shown is for the highest state in the following order: recording, buffering, and off/docked.

Right-click a cluster to show a list of devices in the cluster. The list order is: active devices with alerts, active devices with recently active alerts, recently active devices, and devices that are off.



Because marker location is based on GPS, the accuracy of a camera's location can vary. When the location is selected from the [Recording list](#), the map jumps to the location and the marker shows a blue circle around it, as shown here. The blue circle provides a visual indication of the approximate camera location. The camera is in the circle, but not necessarily in the center.

Navigate the map

- Drag your mouse to move the map.
- Select the map + or – icons (lower right of the map) to zoom in or out, or use your mouse wheel.
- Select **View All Officers** to zoom out to all cameras currently on the map.



Real-time alerts

When an officer takes an action that is configured for notification, the information is passed to Axon Respond as an alert or general officer activity notification.

Actions configured as High Priority Alerts send an alert in real-time and display as a banner at the top of the map.

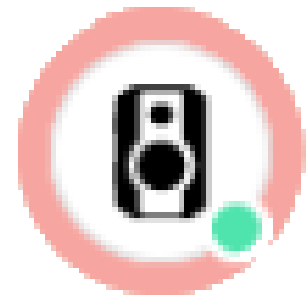


Selecting on the banner takes you to the map location of the alert. Select **X** to dismiss the banner.

The also displays in the Recording list, device marker, and the map marker for the officer as a red ring:

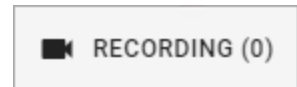
Alerts display in the Recording list, marker, and map for four hours.

Actions configured for General Officer Activity send the information to the Recording list and device marker in the Officer Activity section.



Recording list and user search

The Recording button on the map shows the number of cameras currently recording. Select the button to open the Recording list, which shows a list of names for active or recently active users, vehicles, or devices. Use the Recording list to show the most recent device location and start a livestream. The list is sorted alphabetically with cameras currently recording listed first.



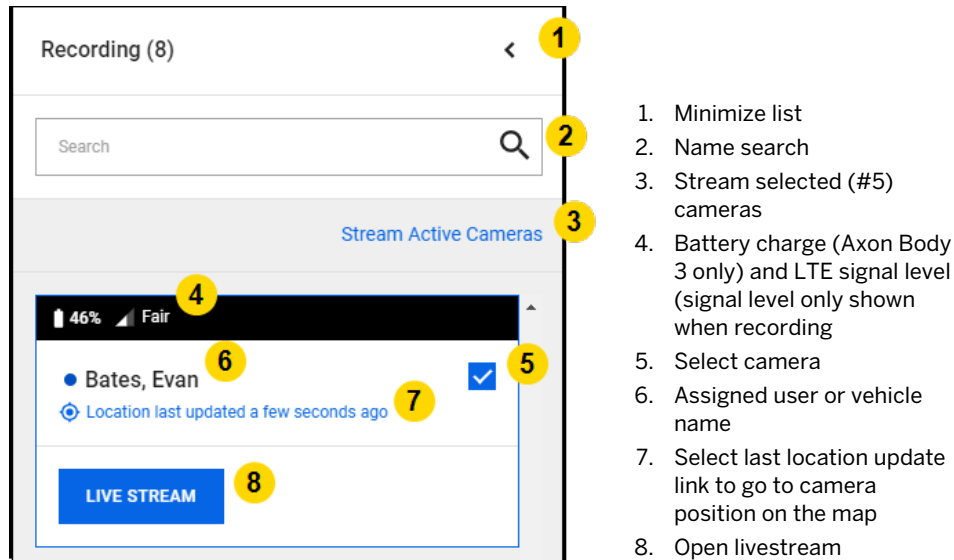
The length of time a marker remains on the map depends on the [Respond Device Location](#) filter setting for your agency.

Livestreaming is only available for Axon Respond+ license users.

- Select location to move the map to the marker location and show the marker information.
- Select **Live Stream** to start a livestream for the selected camera. For Axon Fleet 3, only Dual View is available for livestreaming.
- To open multiple livestreams, select the check box for each camera and then **Stream Active Cameras**.

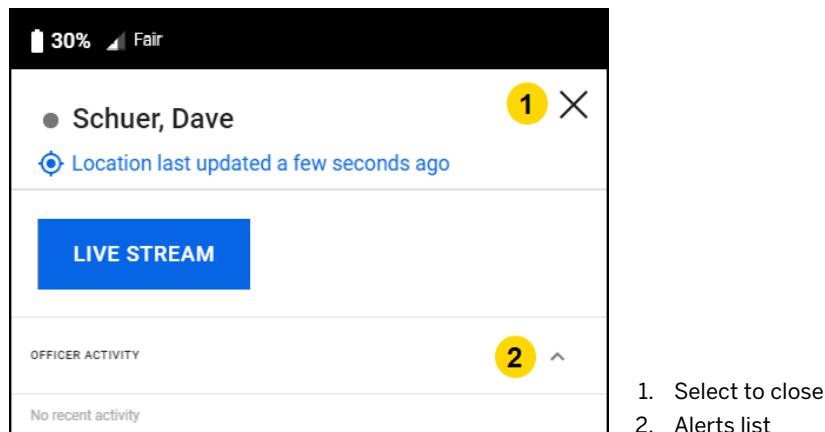


There is also a search box to search by user name.



Device marker information

Select a marker on the map or a location from the Recording list to display device information. If the camera is recording, you can start a livestream.



Livestreaming

While an Axon body, Fleet, or Air camera is recording, its livestream can be viewed in Respond (requires Respond+ license) by up to 25 users simultaneously.

Livestreaming affects body camera battery capacity, reducing charge by approximately an additional 10% for every 30 minutes of livestreaming. Other environmental factors will also affect battery life.

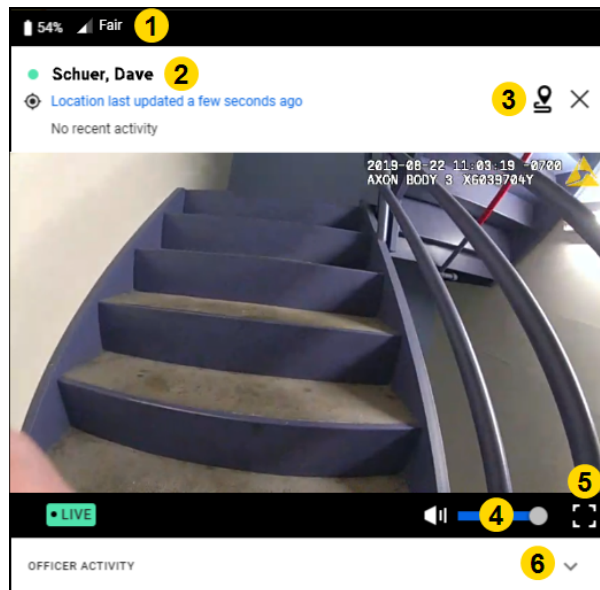
Select a marker on the map or open the Recording list and select **Live Stream** to view a livestream. The button is gray if you are already watching the stream.

Livestream views open on the map above the camera marker. You can have up to 25 views open at a time. Each view lets you control its volume or expand it to full screen.

Livestreaming default ratings are:

- Bit-rate is 1 Mbps for video and 128 Kbps for audio (bit-rate measures the amount of data transmitted in a given amount of time).
- Streaming quality (resolution) is 480p (848x480).
- Frames per second is 30fps.

To move the livestream view window, simply drag it. Each livestream view includes an icon denoting if the window is untethered  (has been moved away from the camera marker) or is still tethered . Selecting the untethered icon teathers the window back to the camera marker.



1. Battery charge and LTE signal level (signal level only shown when recording)
2. User or vehicle name and location
3. Tethered/untethered status; select to close livestream
4. Volume
5. Full screen
6. Alerts list

When a livestream ends or fails due to signal strength or connection issues, a message displays on the livestream viewer.

Audit trail

Any time a livestream is accessed, the action is logged in user and device audit trails.

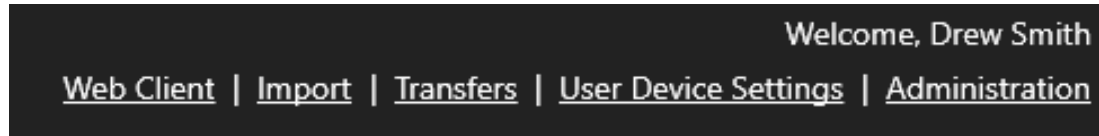
The user audit trail shows the date-time the livestream is accessed and closed, along with the serial number of the camera.

The device audit trail shows the date-time the livestream is accessed and closed.

Manage inventory

This and all remaining sections in this manual are intended for Evidence Local administrators. For user-based topics, start at the [Overview](#) on page 1.

If this is in fact the 'droid you're looking for, select **Administration** from the Quick menu.



If you don't see a tab for **Inventory** on the Administration page, your account requires additional rights.

Overview

The Inventory section lets you view, manage, assign, create, and configure Axon devices for users, but some actions require advanced rights.

Manage device assignment rights let you:

- View, assign, name, and set the port information for Axon body cameras
- Create and modify Vehicle information for Axon Fleet installations

Manage device configuration rights let you:

- View, name, and set the port information for Axon body cameras
- Create and modify vehicle information for Axon Fleet installations
- View information for Axon Signal devices
- Manage device settings

Find inventory information

1. Select **Inventory** from the [Quick menu](#).
2. Select the appropriate tab: [Cameras](#), [Vehicles](#), Signal Devices, or [TASER](#)). TASER includes handles, batteries, and cartridges.
3. Enter filters to narrow the list, then select **Search** to apply.

Cameras

Set a camera name

Naming a camera makes it easier to work with.

1. Select **Inventory** from the [Quick menu](#), then the **Cameras** tab.
2. Use the filters to find the desired camera.
3. Select **Search**.

The screenshot shows the 'Cameras Search' interface. At the top, there are tabs for 'Cameras', 'Vehicles', 'Signal Devices', and 'TASER'. Below the tabs is a search form with fields for 'Model:', 'Serial No.', 'Camera Name:', and 'Assigned To:'. There is also a 'Search' button. Below the search form are two date pickers for 'Last Upload From:' and 'Last Upload To:', and a checkbox for 'Hide deactivated devices'. Below the search form is a table with the following columns: Model, Serial No., Camera Name, Last Upload, Assigned To, Device Status, and Firmware.

Model	Serial No.	Camera Name	Last Upload	Assigned To	Device Status	Firmware
Axon Body 3	X6039705A	X6039705A	12/5/2022 4:17:33 PM	(n/a). admin (commanderadmin)	Assigned	1.3.37
Axon Body 2	X81255708	X81255708	9/20/2021 9:32:33 AM	** Unassigned **	In Stock	1.25.16
Axon Body 2	X81251568	X81251568	9/20/2021 9:32:32 AM	** Unassigned **	In Stock	1.25.16
Axon Body 2	X81255130	X81255130	9/20/2021 8:27:48 AM	Tester, Commander (Tester01)	Review	1.25.16
Axon Body 3	X60FAKE99	X123	8/11/2021 3:18:32 PM	(n/a). admin (commanderadmin)	Assigned	

4. Enter a **Camera Name** for the camera.
5. Press **Enter** or move to any other field to save the change.

Change camera assignment

Requires: **Manage device assignment** right

Files imported or ingested from an assigned device are automatically assigned to its user.

1. Select **Inventory** from the [Quick menu](#), then the **Cameras** tab.
2. Use the filters to find the desired camera.
3. Select **Search**.
4. Select the **Assigned To** field (see prior section for sample screen).
5. Select the user to assign and select **OK**. To unassign a camera, select **Unassigned**. If needed, enter a last name in **Filter** to narrow down the list.

The screenshot shows a 'Pick User' dialog box. It has a title bar with a close button. Below the title bar is a section labeled 'Options:' containing a list of users. The first option is '** Unassigned **'. The second option is 'Smith, Drew (cdr111)' and is highlighted. The third option is 'Jones, John (cdr75)'. Below the list is a 'Filter:' field with a text input box. At the bottom of the dialog box is an 'OK' button.

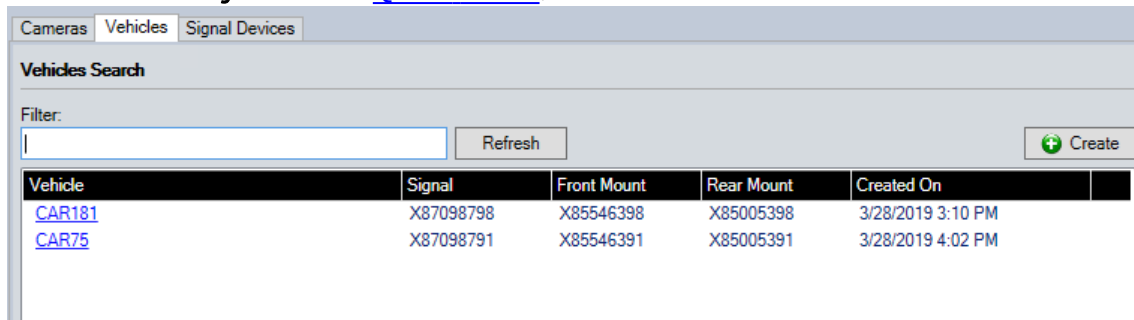
6. Confirm the change. The change in assignment status appears at the lower right side of the page.

Vehicles

Add a vehicle

Vehicle information is used with Axon Fleet installations. Each vehicle must be configured in Evidence Local before the associated Axon View XL application can connect to the system and upload videos from Axon Fleet cameras. The mobile data terminal (MDT) or mobile digital computer (MDC) in the vehicle uses the Wi-Fi configuration (SSID and password) information to connect to the system.

1. Select **Inventory** from the [Quick menu](#), then the **Vehicles** tab.



The screenshot shows the 'Vehicles Search' interface. At the top, there are tabs for 'Cameras', 'Vehicles', and 'Signal Devices'. Below the tabs is a 'Filter:' input field and a 'Refresh' button. To the right is a '+ Create' button. The main area contains a table with the following data:

Vehicle	Signal	Front Mount	Rear Mount	Created On
CAR181	X87098798	X85546398	X85005398	3/28/2019 3:10 PM
CAR75	X87098791	X85546391	X85005391	3/28/2019 4:02 PM

2. Select **Create**.



The screenshot shows the 'Create a Vehicle' dialog box. On the left is a diagram of a vehicle with a camera and signal device. On the right, there are three steps to complete:

- Vehicle Name:** [Text input field]
- Step 1. Assign Signal Vehicle Device**
Serial No. : [Text input field]
- Step 2. Assign Front and Rear Power Units**
Front Serial No. : [Text input field]
Rear Serial No. : [Text input field]
- Step 3. Configure Wi-Fi**
SSID: [Text input field]
Password: [Text input field]
☒ Show Password

At the bottom are 'Create' and 'Cancel' buttons.

3. Enter a **Vehicle Name**.
4. Enter the **Serial number** for the Axon Signal Vehicle device installed in the vehicle. These serial numbers for always begin with X87.

5. Enter the **Serial numbers** for the Axon Fleet Power Units associated with the Fleet front and back cameras.
6. Enter the Wi-Fi **SSID** and **Password** for the system (both fields are case-sensitive).
7. Select **Create**. The vehicle information is added to the Vehicles tab.

Edit vehicle information

1. Select **Inventory** from the [Quick menu](#), then the **Vehicles** tab.

Vehicle	Signal	Front Mount	Rear Mount	Created On
CAR181	X87098798	X85546398	X85005398	3/28/2019 3:10 PM
CAR75	X87098791	X85546391	X85005391	3/28/2019 4:02 PM

2. **Filter** to find the desired vehicle.
3. Select the vehicle.
4. Enter the updated information in the appropriate fields (see sample screen in the prior section). You can leave fields blank if appropriate.

Note The Wi-Fi fields are case-sensitive.

5. Select **Modify**. The updated vehicle information displays on the Vehicles tab.

TASER, change assignment

Requires: **Manage device assignment** right

Files imported or ingested from an assigned device are automatically assigned to its user.

Note You can only assign TASER device handles.

1. Select **Inventory** from the [Quick menu](#), then the **TASERS** tab.

The screenshot shows the 'TASER Search' interface. At the top, there are tabs for 'Cameras', 'Vehicles', 'Signal Devices', and 'TASER'. Below the tabs, there is a search form with fields for 'Model:', 'Serial No.', 'Assigned To:', and 'Device Health:'. The 'Model:' dropdown is set to 'TASER 7 Handle'. There is a 'Search' button and checkboxes for 'Not assigned' and 'Hide deactivated devices'. Below the search form is a table with 7 rows of device information.

Model	Serial No.	Assigned To	Device Health	Device Status	Firmware	Log Update Time
TASER 7 Handle	X40002P01	** Unassigned **	Good	In Stock	1.8.3	9/29/2021 12:14:32 PM
TASER 7 Handle	X4000C4YR	** Unassigned **	Good	In Stock	1.7.2	8/11/2021 4:31:30 PM
TASER 7 Handle	X410020AV	** Unassigned **	Good	In Stock	1.7.2	6/15/2021 7:12:09 AM
TASER 7 Handle	X410020AP	** Unassigned **	Good	In Stock	1.7.2	6/15/2021 6:42:50 AM
TASER 7 Handle	X41002053	** Unassigned **	Good	In Stock	1.7.2	6/15/2021 4:45:16 AM

7 of 20 TASER devices are displayed.

2. Use the filters to find the desired TASER.
3. Select **Search**.
4. Select the **Assigned To** field for the desired TASER.
5. Select the user to assign and select **OK**. To unassign a camera, select **Unassigned**. If needed, enter a last name in **Filter** to narrow down the list.

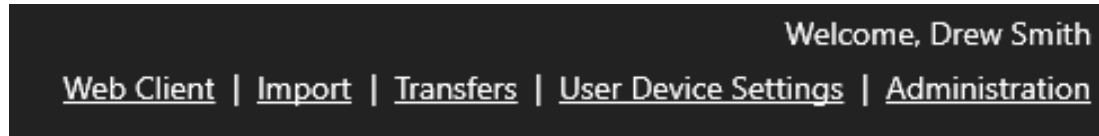
The screenshot shows a 'Pick User' dialog box. It has a title bar with a close button. Below the title bar, there is a section labeled 'Options:' with a list of users. The first option is '** Unassigned **'. The second option is 'Smith, Drew (cdr111)' and is highlighted. The third option is 'Jones, John (cdr75)'. Below the list is a 'Filter:' section with a text input field. At the bottom of the dialog is an 'OK' button.

6. Confirm the change. The change in assignment status appears at the lower right side of the page.

Manage users

This and all remaining sections in this manual are intended for Evidence Local administrators. For user-based topics, start at the [Overview](#) on page 1.

If this is in fact the 'droid you're looking for, select **Administration** from the Quick menu.



If you don't see a tab for **Users** on the Administration page, your account requires additional rights.

Overview

Evidence Local supports two types of users:

- **Evidence Local Users** are added, authenticated, and managed by the Evidence Local application.
- **Active Directory Users** are registered with Evidence Local, but authentication takes place on an agency's Active Directory Server. Validation of an Active Directory User is always sent to the Active Directory Server; Evidence Local never stores Active Directory User passwords or other data contained in Active Directory. Active Directory users are added when the Active Directory Group they belong to is added to Evidence Local (see [Add a group from Active Directory](#) on page 61). Use Evidence Local Checkup to update Active Directory Users. Active Directory User domain names appear before their user name in the user list.

This article discusses how to manage Evidence Local users.

Add a user

1. Select **Administration** from the [Quick menu](#) (page 3), then the **Users** tab. The first user listed should be the default admin.
2. In the **User Properties** dialog box, select **Add**.

3. In the **User Properties** dialog box, enter the user's information.

The image shows the 'User Properties' dialog box with the 'New User' tab selected. The 'Information' sub-tab is active, displaying several input fields: 'User ID', 'Full Name' (split into 'First', 'MI', and 'Last' sections), 'Username', 'E-mail', and 'Modified At' (showing '(unknown)'). Below these is a 'Password' section with 'New Password' and 'Confirm Password' fields. At the bottom, there are two checkboxes: 'Enable User Account' (checked) and 'User must change password at next logon' (unchecked). The dialog has 'OK', 'Close', and 'Apply' buttons at the bottom right.

- **User ID** – A unique ID for the user. Use as a Badge ID or Employee ID. Accepts a string input.
 - **Full Name** – The user's First Name, Middle Initial, and Last Name. This information is used for showing file ownership and displays in the upper right corner of Evidence Local after the user logs in.
 - **Username** – A unique username for the user. Used for sign-in and device assignments.
 - **E-mail** – The user's e-mail address.
 - **New Password/Confirm Password** – The user's password.
 - **Enable User Account** – This is selected by default. Clear to disable the user's account.
 - **User must change password at next logon** – Requires the user to change their password the next time they sign in.
4. Select **Apply** to add the user.
5. Provide the user with their username and password so they can sign in.
6. Select **Close** to exit.

Edit a user

1. Select **Administration** from the [Quick menu](#), then the **Users** tab.
2. Use the filters to find the desired user.
3. Double-click the user row.
4. In the **User Properties** dialog box, edit the user information as needed.

Note Clearing the **Enable User Account** checkbox disables the user's account but keeps it available for later use.

5. Select **Apply** to save the changes.
6. Select **Close** to exit.

Force a password change

This requirement will take effect the next time the user signs in.

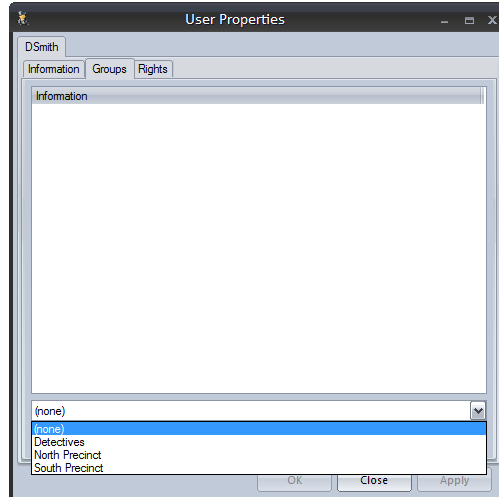
1. Select **Administration** from the [Quick menu](#), then the **Users** tab.
2. Use the filters to find the desired user, then double-click the row.
3. Select the **User must change password at next logon** checkbox.
4. Select **Apply** to save the changes.

Assign a user to a group

When you place users into groups that have a designated role within the system, such as a group for detectives or administrators, you can assign rights at a group level that its members inherit, much like in Microsoft Windows. For details on creating a group, see [Manage groups](#) on page 60.

1. Select **Administration** from the [Quick menu](#), then the **Users** tab.
2. Use the filters to find the desired user, then double-click the row.
3. To add the user to a group:
 - a. In the **User Properties** dialog box, select the **Groups** tab. Any groups the user already belongs to are listed here.

- b. Select the group from the drop-down list at the bottom.

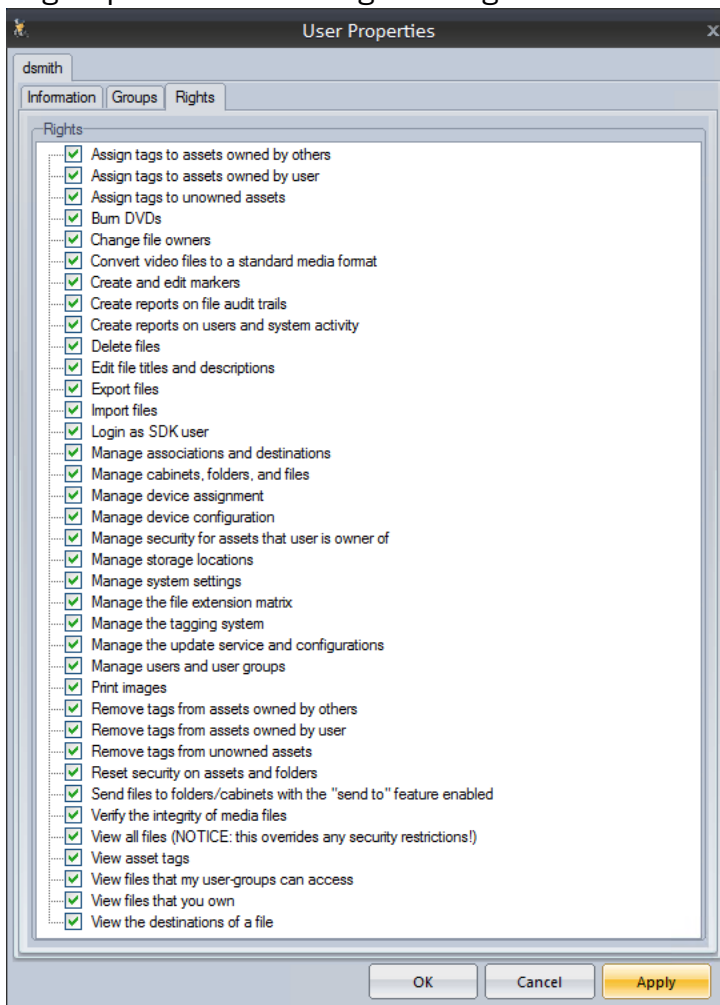


- c. Select **Add** to add the group to the list.
 - d. Repeat the prior step to add another group.
4. To remove a user from a group:
 - a. Select the group in the list.
 - b. Select **Remove**.
 - c. Repeat the prior step to remove another group.
 5. Select **Apply** to save all the group changes.
 6. Select **Close** to exit.

Set user rights

All users in Evidence Local, whether registered as users of Evidence Local or Active Directory, have a set of assigned rights. Use rights to allow or restrict users from

performing certain actions in Evidence Local. User can inherit rights by being assigned to groups that have the rights assigned.

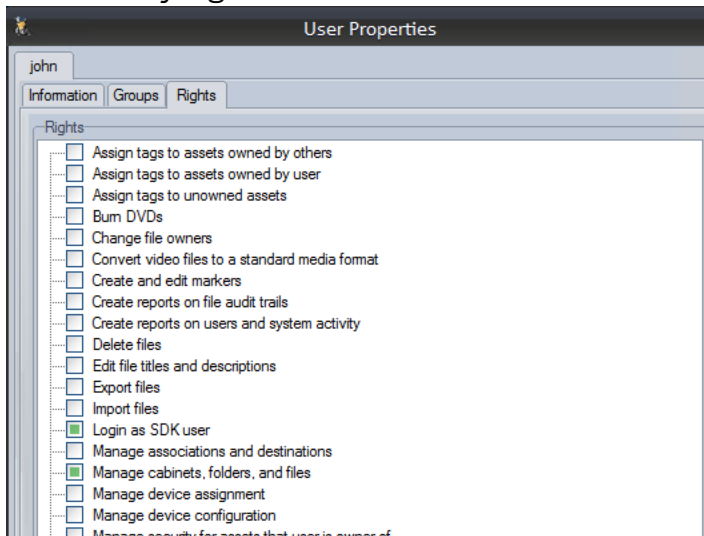


1. Select **Administration** from the [Quick menu](#), then the **Users** tab.
2. Use the filters to find the desired user, then double-click the row.
3. In the **User Properties** dialog box, select the **Rights** tab.
4. Select the checkbox for each right you want to assign. Clear the checkboxes for rights you don't want to assign (see [List of user rights](#) on page 57).
5. Select **Apply** to save the changes.
6. Select **Close** to exit.

Inherit rights from a group

Users assigned to a group inherit the rights assigned to that group. For example, if the Group has the **Burn DVDs** right selected, all users assigned to that group also have that right.

On the rights tab of the **User Properties** dialog box, rights inherited from a group are indicated by a green box inside the checkbox.



When a user belongs to multiple groups, this tab shows the inherited rights for all groups combined.

List of user rights

These are the different user rights available. In most cases, the name is self-explanatory.

Assign tags to assets owned by others – Lets the user add tags to files owned by other users.

Assign tags to assets owned by user – Lets the user add tags to files owned by the user.

Assign tags to unowned assets – Lets the user add tags to files are not owned by any user.

Burn DVDs – Lets the user use the *Burn to DVD* operation.

Change File owners – Lets the user change the file owner (Primary User and Secondary User) in the File Properties dialog box.

Convert video Files to a standard media format – Allows users to use the *Convert to standard media* operation.

Create and edit markers – Lets the user create and edit markers for audio and video files in the player.

Create Reports on file audit trails – Lets the user use the *Create Report* operation.

Create Reports on users and system activity – Lets the user run detailed user and system activity.

Delete files – Lets the user delete files.

Delete markers – Lets the user delete markers from a file.

Edit file titles and descriptions – Lets the user edit file titles and descriptions from the File Properties dialog box.

Export Files – Lets the user use the Export File operation.

Import Files – Lets the user access the Import section.

Log in to ViewXL – Lets the user sign into the Axon View XL application for the Axon Fleet in-car system.

Manage Air integration – Lets the user set up integration with Air devices.

Manage associations and destinations – Lets the user manage and control association rules and destinations in Administration.

Manage Cabinets, Folders, and Files – Lets the user manage and control folders and cabinets in Administration.

Manage device assignment – Lets the user assign and unassign Axon devices, such as cameras, in Administration and through the Axon Device Manager (ADM) mobile app.

Manage device configuration – Lets the user define the camera settings for Axon body worn cameras.

Manage device status – Lets the user change device names or modify device settings, such as speaker volume and indicator lights.

Manage security for assets that user is owner of – Lets the user allow or restrict other users from viewing assets they own. This lets users control access to their own files from the asset Properties > Security tab without having the global *Manage Cabinets, Folders, and Files* right.

Manage storage locations – Lets the user manage and control storage locations in Administration.

Manage system settings – Lets the user manage and control system settings in Administration.

Manage the File Extension matrix – Lets the user manage and control the file extension matrix in Administration.

Manage the Tagging system – Lets the user manage and control tags in Administration.

Manage the Update service and configurations – Lets the user manage and control the Installation, Installation Groups, and Updates sections in Administration.

Manage Users and User Groups – Lets the user manage and control users and groups in Administration.

Print images – Lets the user send image files to a printer.

Remove tags from assets owned by others – Lets the user remove tags from files owned by other users.

Remove tags from assets owned by user – Lets the user remove tags from files owned by the user.

Remove tags from unowned assets – Lets the user remove tags from files that are not owned by any user.

Reset security on assets and Folders – Lets the user reset security on all folders and files within a cabinet hierarchy.

Respond live stream – Lets the user view livestreams from the Axon Respond map.

Respond view audit log – Lets the user export the Axon Respond audit log.

Respond view location map – Lets the user open and view the Axon Respond map.

Send Files to Folders/Cabinets with the "Send to" feature enabled – Lets the user use the *Send To* operation.

Take devices from pool – Lets the user take an Axon body-worn camera with device pooling.

TASER reporting and allocation – Lets the user run and download TASER reports.

Verify the File integrity of media Files – Lets the user use the *Verify File Integrity* operation.

View all Files – Lets the user view any file, regardless of other restrictions.

View asset tags – Lets the user view the tags associated with a file.

View Files that my User Groups can access – Lets the user search for and access any file their groups have access to through security configurations.

View Files that other users in my User Groups own – Lets the user search for and access any file that any user with the same user group owns.

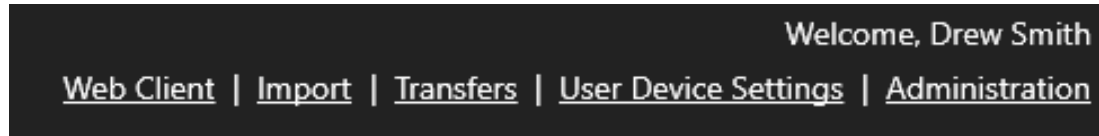
View Files that you own – Lets the user search for and access files they own.

View destinations of a File – Lets the user view file destinations (files sent to and received from other Evidence Local systems).

Manage groups

This and all remaining sections in this manual are intended for Evidence Local administrators. For user-based topics, start at the [Overview](#) on page 1.

If this is in fact the 'droid you're looking for, select **Administration** from the Quick menu.



If you don't see a tab for **Groups** on the Administration page, your account requires additional rights.

Overview

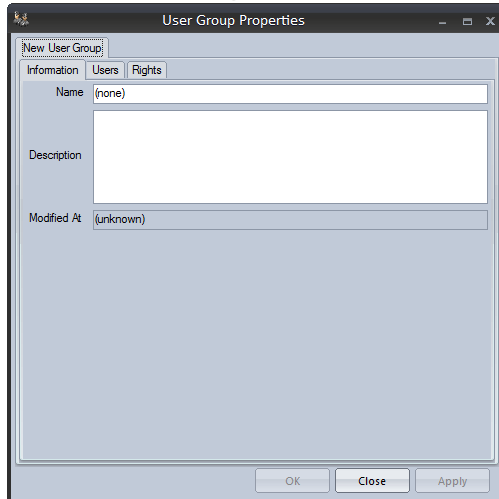
Groups provide an easy way to assign and manage the same rights and file access to multiple users at the same time. With groups, you don't need to assign rights to each user in the system; assign the right to a group, then add the user to that group. Groups can be created in Active Directory and then added to Evidence Local.

Add a group

1. Select **Administration** from the [Quick menu](#) (page 3), then the **Groups** tab.
2. In the **User Group** dialog box, select **Add** at the bottom right.

Note If your Evidence Local instance is connected to Active Directory, the **Add new user-group** dialog box opens. To add a non-Active Directory group, select **Create (non-Active Directory) Evidence Local group** and continue with this procedure. See [Add a group from Active Directory](#) on page 61) for information on adding an Active Directory group.

3. Create the new group in the User Group Properties dialog box:



- **Name** – The name of the group
 - **Description** – A useful description of the group
4. Select **Apply**.
 5. Select **Close** to exit.

Edit a group

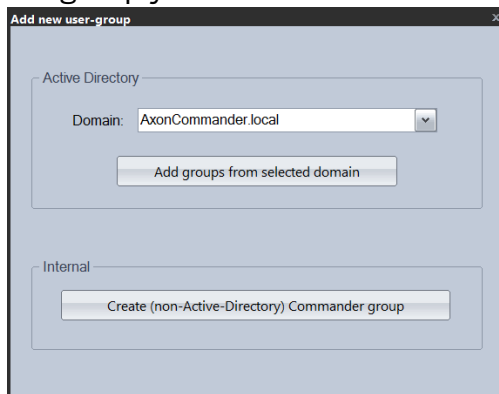
1. Select **Administration** from the [Quick menu](#), then the **Groups** tab.
2. Use the filters to find the desired group.
3. Double-click the group row.
4. In the User Group Properties dialog box, edit the group information as needed. You can't edit the Name and Description of Active Directory groups.
5. Select **Apply** to save the changes.
6. Select **Close** to exit.

Add a group from Active Directory

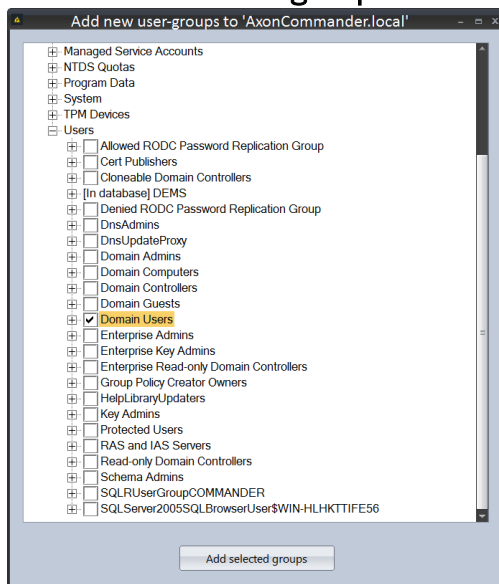
Groups managed in Active Directory can be added into Evidence Local Administration.

1. Select **Administration** from the [Quick menu](#), then the **Groups** tab.
2. Select **Add** at the bottom right of the window.

3. In the **Add new user-group** dialog box, select the Active Directory Domain with the group you want to add.



4. Select **Add groups from selected domain**.
5. Expand the Domain and Users lists, select the group(s) you want to add, then select **Add selected groups**.

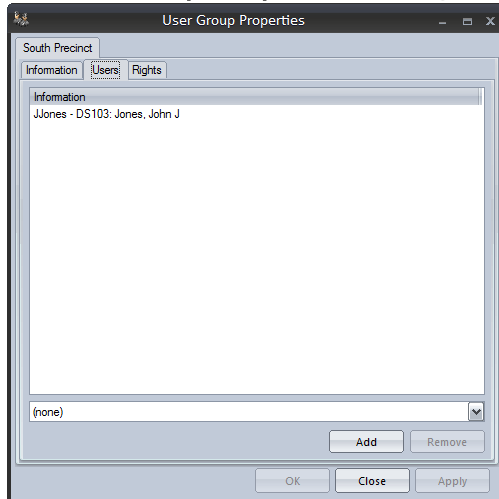


6. Select **OK** to acknowledge the addition.

Assign users to a group

1. Select **Administration** from the [Quick menu](#), then the **Groups** tab.
2. Use the filters to find the desired group.
3. Double-click the group row.

4. In **User Group Properties** dialog box, select the **Users** tab.



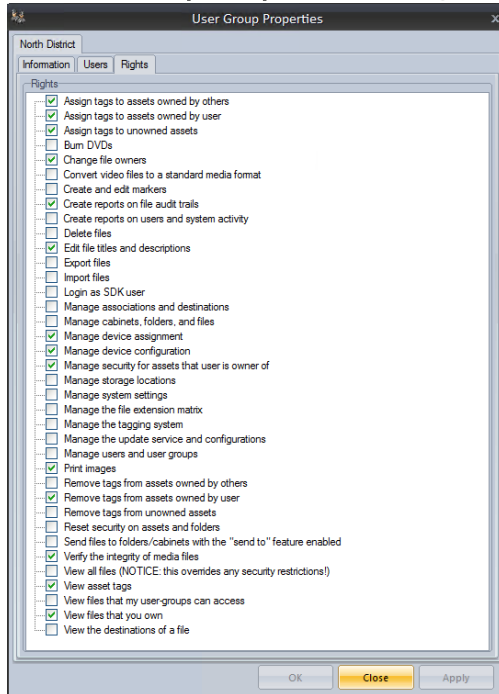
5. To add a user to the group:
 - a. Select the user from the dropdown box at the bottom.
 - b. Select **Add**.
 - c. Repeat to add another user.
6. To remove a user from the group:
 - a. Select the user in the list.
 - b. Select **Remove**.
 - c. Repeat this step to remove another user.
7. Select **Apply** to save the changes.

Set group rights

Group rights are the same as user rights, except the group rights apply to all users assigned to the group.

1. Select **Administration** from the [Quick menu](#), then the **Groups** tab.
2. Use the filters to find the desired group.
3. Double-click the group row.

4. In **User Group Properties** dialog box, select the **Rights** tab.

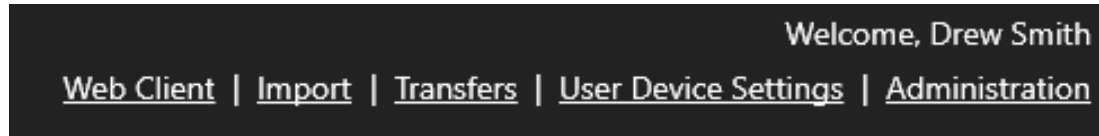


5. Select the checkboxes for the rights you want to assign to the group. For details on each right, see [List of user rights](#) on page 57 on page 57
6. Clear the checkboxes adjacent to the rights you don't want the group to have.
7. Select **Apply** to save the changes.
8. Select **Close** to exit.

Manage folders

This and all remaining sections in this manual are intended for Evidence Local administrators. For user-based topics, start at the [Overview](#) on page 1.

If this is in fact the 'droid you're looking for, select **Administration** from the Quick menu.



If you don't see a tab for **Folders** on the Administration page, your account requires additional rights.

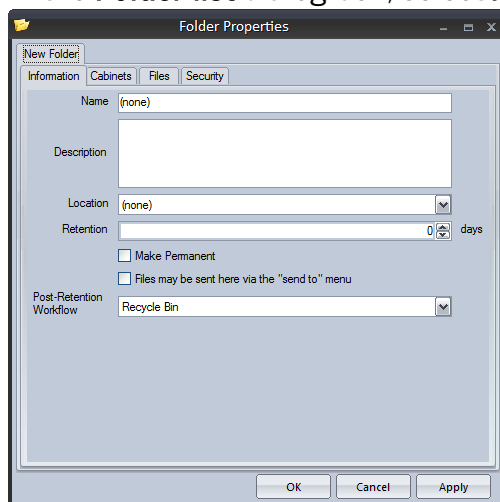
Overview

Folders are virtual containers for categorizing files. Use folders to set retentions (how long a file is saved), manage where the files are physically stored on the network, and set access control. Files can be associated with multiple folders.

Association rules can be created to automatically place files into folders when they are ingested or as specific metadata, such as markers, tags, or assigned users, is placed on the file.

Add a folder

1. Select **Administration** from the [Quick menu](#) (page 3), then the **Folders** tab.
2. In the **Folder list** dialog box, select **Add** at the bottom right.



3. In the **Folder Properties** dialog box, enter a clear and easily understandable folder **Name**.
4. Enter a **Description** for the folder.
5. Select the storage **Location** for the folder.
6. Enter the **Retention** time in days. This is how long a file should be kept in the folder before being removed from the system. The value must be greater than zero.
7. If files should not be removed from the folder, select **Make Permanent**. Folders marked as such don't require a Retention time and their files are never removed.
8. Select **Files may be sent here via the "send to" menu** if users with the **Send Files to Folders/Cabinets with the Send To feature** right can associate files with this folder with the [context-sensitive](#) (page 11) menu option.
9. Select the **Post Retention Workflow** destination for files. This workflow transfers files to the specified location when the Retention time for the folder is reached and the file is not associated with any other folder with a greater retention time. The default setting is the Recycle Bin. The Recycle Bin cannot be deleted and is used to catch files in case of an accidental deletion. By default, the Recycle Bin has **Make Permanent** selected, but this can be changed by editing the Recycle Bin folder (see next section).
10. Select **Apply** to save the settings.

Edit a folder

1. Select **Administration** from the [Quick menu](#), then the **Folders** tab.
2. In the **Folder list** dialog box, use the filters to find the desired folder.
3. Double-click the folder row.
4. In the Folder Properties dialog box, edit the folder information as needed.
5. Select **Apply** to save the changes.
6. Select **Close** to exit.

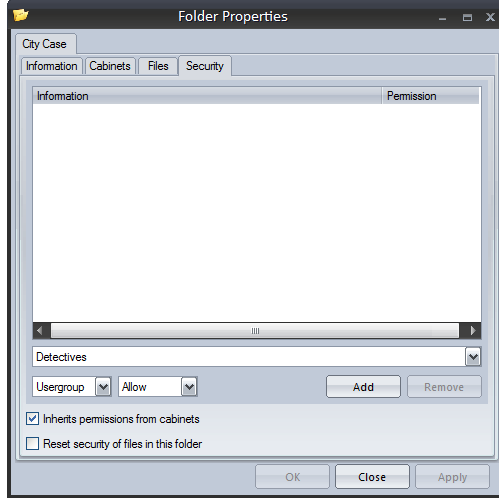
Set folder access control

Use access control to set the access options for users and groups. Access to a folder and all files associated with it can be allowed or restricted.

Note Ensure your users have the **View Files that my User-Groups can access** right enabled. Without it, they won't be able to access files even if a group they are part of is allowed access to the folder.

1. Select **Administration** from the [Quick menu](#), then the **Folders** tab.
2. In the **Folder list** dialog box, use the filters to find the desired folder.
3. Double-click the folder row.

4. In the **Folder Properties** dialog box, select the **Security** tab, which lists user and group access control (Allowed and Restricted) rules for the folder. The list is blank if this is the first time you are assigning access control to a folder.



5. Set access control rules:
 - a. **User/group selection list** – Selects the specific user or group to which the access control applies (here, *Detectives*). Whether users or groups is shown in the list is determined by the User/Usergroup list below it.
 - b. **User/usergroup list** – Sets if the User/Group Selection list above it shows a list of users or groups (here, *Usergroup*).
 - c. **Allow/restrict list** – Sets the enter of access control (here, *Allow*). If **Allow**, the user or group is allowed access to the folder. If **Restrict**, then no.
 - d. **Inherits permissions from cabinets** – Sets the access control settings to be inherited from a parent cabinet. This is selected by default. For details, see [Set cabinet access control](#) on page 71 on page 71.
 - e. **Reset security of files in this folder** – Sets the access control setting for any files associated with the folder to the access control settings of this folder.
6. Once settings are complete, select **Add** to add the folder access rule.
7. After adding all needed rules for the folder, select **Apply** to save the changes.

Remove folder access

1. Select **Administration** from the [Quick menu](#), then the **Folders** tab.
2. In the **Folder list** dialog box, use the filters to find the desired folder.
3. Double-click the folder row.
4. In the **Folder Properties** dialog box, select the **Security** tab.
5. Select the user or group to remove from the list.
6. Select **Remove**.

7. Select **Apply** to save the change.
8. Select **Close** to exit.

Associate folders with cabinets

1. Select **Administration** from the [Quick menu](#), then the **Folders** tab.
2. In the **Folder list** dialog box, use the filters to find the desired folder.
3. Double-click the folder row.
4. In the **Folder Properties** dialog box, select the **Cabinets** tab.
5. Select **Add**.
6. Use the filters to find the cabinet you want to associate with the folder.
7. Hold the Ctrl key to select multiple cabinets at once.
8. Select **OK** to add the selected cabinets to the list.
9. Select **Apply** to save the changes.
10. Select **Close** to exit.

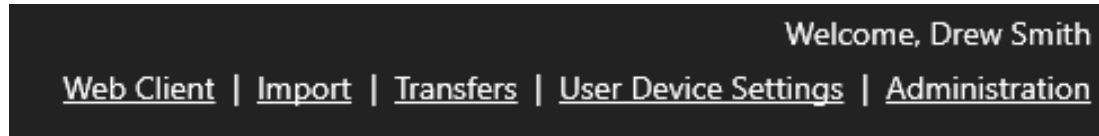
Folder properties Files tab

The **Files** tab in the **Folder Properties** dialog box shows a list of files currently associated with the folder. This list is for viewing only.

Manage cabinets

This and all remaining sections in this manual are intended for Evidence Local administrators. For user-based topics, start at the [Overview](#) on page 1.

If this is in fact the 'droid you're looking for, select **Administration** from the Quick menu.



If you don't see a tab for **Cabinets** on the Administration page, your account requires additional rights.

Overview

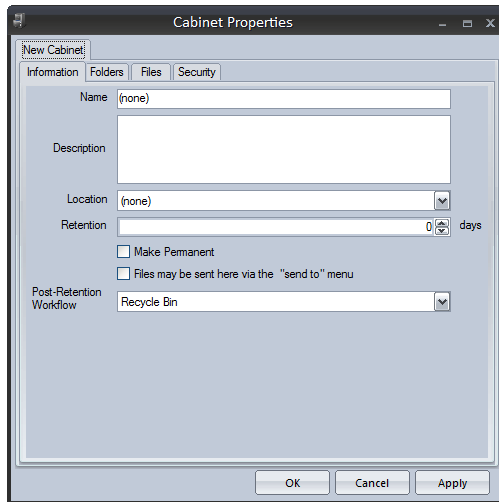
Cabinets are the highest organizational structure for setting access control rules and retention times for files in Evidence Local. [Folders](#) are organizational structures that can be associated with cabinets. Files in Evidence Local can be managed solely with folders, but cabinets help organize a large amount of distinct organizational structures within your system. This allows for more granularity when setting up access control rules and retention times.

Files can be directly associated with cabinets. However, best practice is to associate files with folders and associate folders with cabinets.

Add a cabinet

1. Select **Administration** from the [Quick menu](#), then the **Cabinets** tab.
2. Beneath the list of cabinet names and descriptions, select **Add**.

3. In the **Cabinet Properties** window, enter a clear and easily understandable **Name** for the cabinet.



4. Enter a **Description** for the cabinet.
5. Select the storage **Location** for the cabinet.
6. Enter the **Retention** time in days. This is how long a file should be kept in the cabinet before being removed from the system. The value must be greater than zero. Retention times are inherited by all folders associated with the cabinet.
7. If files should not be removed from the cabinet, select **Make Permanent**. Cabinets marked as such don't require a Retention time and their files are never removed.
8. Select **Files may be sent here via the "send to" menu** if users with the **Send Files to Folders/Cabinets with the Send To** feature right can associate files with this cabinet with the [context-sensitive](#) (page 11) menu option.
9. Select the **Post Retention Workflow** destination for files. This workflow transfers files to the specified location when the Retention time for the cabinet is reached and the file is not associated with any other cabinet with a greater retention time. The default setting is the Recycle Bin. The Recycle Bin cannot be deleted and is used to catch files in case of an accidental deletion. By default, the Recycle Bin has **Make Permanent** selected, but this can be changed by editing the Recycle Bin folder (see next section).
10. Select **Apply** to save the settings.

Edit a cabinet

1. Select **Administration** from the [Quick menu](#), then the **Cabinets** tab.
2. In the **Cabinet list** dialog box, use the filters to find the desired folder.
3. Double-click the cabinet row.
4. In the Cabinet Properties dialog box, edit the cabinet information as needed.

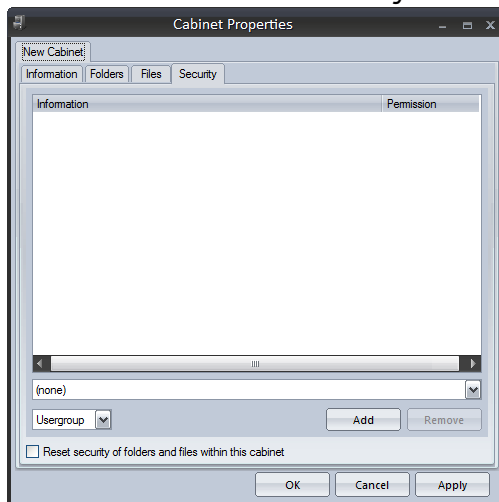
5. Select **Apply** to save the changes.
6. Select **Close** to exit.

Set cabinet access control

Use access control to set the access options for users and groups. Access to a cabinet and all files and folders associated with it can be allowed or restricted.

Note Ensure your users have the **View Files that my User-Groups can access** right enabled. Without it, they won't be able to access files even if a group they are part of is allowed access to the cabinet.

1. Select **Administration** from the [Quick menu](#), then the **Cabinets** tab.
2. In the **Cabinet list** dialog box, use the filters to find the desired folder.
3. Double-click the folder row.
4. In the **Cabinet Properties** dialog box, select the **Security** tab, which lists user and group access control (Allowed and Restricted) rules for the cabinet. The list is blank if this is the first time you are assigning access control to a cabinet.



5. Set access control rules:
 - a. **User/group selection list** – Selects the specific user or group to which the access control applies (here, *none*). Whether users or groups is shown in the list is determined by the User/Usergroup list below it.
 - b. **User/usergroup list** – Sets if the User/Group Selection list above it shows a list of users or groups (here, *Usergroup*).
 - c. **Reset security of folders and files within this cabinet** – Sets the access control setting for any files associated with the cabinet to the access control settings of this cabinet.
6. Once settings are complete, select **Add** to add the cabinet access rule.
7. After adding all needed rules for the cabinet, select **Apply** to save the changes.

Remove cabinet access

1. Select **Administration** from the [Quick menu](#), then the **Cabinets** tab.
2. In the **Cabinet list** dialog box, use the filters to find the desired cabinet.
3. Double-click the cabinet row.
4. In the **Cabinet Properties** dialog box, select the **Security** tab.
5. Select the user or group to remove from the list.
6. Select **Remove**.
7. Select **Apply** to save the change.
8. Select **Close** to exit.

Add folders to cabinets

1. Select **Administration** from the [Quick menu](#), then the **Cabinets** tab.
2. In the **Cabinet list** dialog box, use the filters to find the desired cabinet.
3. Double-click the cabinet row.
4. In the **Cabinet Properties** dialog box, select the **Folders** tab.
5. Select **Add**.
6. Use the **Find** field to find the folder you want to associate with the cabinet.
7. Hold the Ctrl key to select multiple folders at once.
8. Select **OK** to add the selected folders to the list.
9. Select **Apply** to save the changes.
10. Select **Close** to exit.

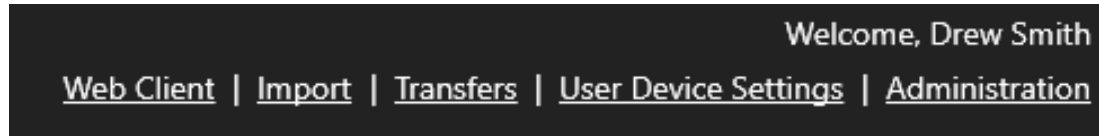
Cabinet properties Files tab

The **Files** tab in the **Cabinet Properties** dialog box shows a list of files currently associated with the cabinet. This list is for viewing only.

Manage tags

This and all remaining sections in this manual are intended for Evidence Local administrators. For user-based topics, start at the [Overview](#) on page 1.

If this is in fact the 'droid you're looking for, select **Administration** from the Quick menu.



If you don't see a tab for **Tags** on the Administration page, your account requires additional rights.

Overview

Use tags to add important metadata information to files. Administrators must create tag templates before users can apply tags. Tag templates can either be Choice tag or Text tag.

- **Choice** tags provide a list of predefined values a user can apply to the file.
- **Text** tags prompt the user to enter a length -constrained free-form text string to place on the file.

Tags are also used in the Association matrix rules to apply metadata to a file, and tag information can be searched.

The tag system lets you to add any type of categorization to files managed by Evidence Local per you agency's need.

When first setting up a tag system, you might want to create a Case ID tag, an Evidence ID tag, and a Choice tag for all Violation types for your agency, then maybe one for Department classifications. The tags you create depends on the expected usage.

Tags are used in association rules. Setting up appropriate tag templates can make your life as an administrator much easier.

Create a tag template

1. Select **Administration** from the [Quick menu](#), then the **Tag** tab. A list of tag templates appears with the following columns:
 - **Name** – The name of the tag template.
 - **Description** – A short description of the tag template.

- **Type** – The enter of the tag template: Text or Choice.
 - **Extra Information** – This shows the length and Regex pattern for a text tag or the number of choices for a Choice tag.
2. Select **Add**. In the **Tag Properties** dialog box:

- Enter a **Name** for the template.
- Enter a **Description** for the template.
- Select the **Type** of template.
 - For Text tag templates:
 - Set the **Min length**.
 - Set the **Max length**.
 - Select if the tag uses **Multiple lines**.
 - Optionally, enter a **Matching pattern** (regex) and **Pattern name**.
 - Set the **Default value**. Normally this will be left blank.
 - For Choice tag templates:
 - Select **Add**.
 - Enter the choice and select **OK**.
 - Repeat the previous two actions until all choices are added.
 - Use the **Up** and **Down** buttons to move the positions of the choices.
- Select the **Options** tab and set the options for this template.
 - **Allow tag template to be transferred** – Files with this tag that are sent to another Evidence Local server using [associations](#) will retain this tag. The destination server must have the tag field available. This causes the tag value on the destination server to be populated with the value from the source server.
 - **Enforce tag on import** – This tag enter must be specified for every file imported through the Import section.

- **Require tag validation** – The user must enter or select the value for this tag type twice while adding a new tag value (either in the Import section or when tagging an existing file). This limits the chance of a tagging error being made.
 - **Show tags** – This tag type displays in the Import section tag list. If not selected, it is hidden.
 - **Assign tags** – This tag type can be applied to files in the Import section.
 - **Show tags** – This tag type displays in the Assets info pop-up window and tags dialog box. If not selected, it is hidden.
 - **Assign tags** – This tag type is available to be applied to files in the tags dialog box.
 - **Edit tags** – Users can edit the value for this tag type in the tags dialog box after the tag was added.
 - **Allow tag removal** – This tag type can be removed from a file in the tags dialog box.
 - **Show in filter (choice tags only)** – This tag type displays in the tags filter list of the Search pane.
7. Select **Apply** to save the changes and add the template to the list.
 8. Select **Close**.

You can't delete a tag template if it is associated with anything.

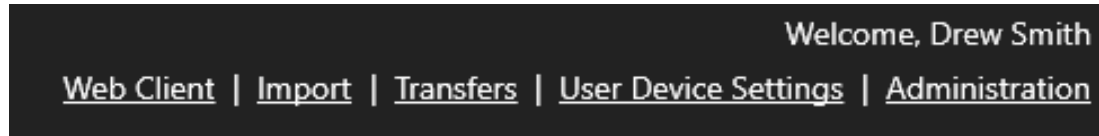
Edit a tag template

1. Select **Administration** from the [Quick menu](#), then the **Tags** tab.
2. In the **Tags** dialog box, use the filters to find the desired tag template.
3. Double-click the tag template row.
4. In the **Tag Properties** dialog box, edit the tag information as needed.
5. Select **Apply** to save the changes.
6. Select **Close** to exit.

Manage associations

This and all remaining sections in this manual are intended for Evidence Local administrators. For user-based topics, start at the [Overview](#) on page 1.

If this is in fact the 'droid you're looking for, select **Administration** from the Quick menu.



If you don't see a tab for **Associations** on the Administration page, your account requires additional rights.

Overview

A workflow rule that automatically places files in an organizational structure (a folder or cabinet) and securely moves them about the network (to a destination) when certain conditions are met is called an **association**. Associations are extremely powerful tools for automating file transfers and movement in Evidence Local.

When Evidence Local physically moves files, it follows all IACP standards for transferring data from location to location, calculating an SHA-2 hash of every file (pre-move and post-move or copy) and auditing all transfers that take place.

An association always contains at least one **constraint**—the condition checked to determine if the rule is triggered—and a **location** where the file is sent when that condition is met. A constraint can be based on areas, markers, sources, tags, and users. The location where the file is sent can be a folder, cabinet, or destination.

An association can have multiple constraints and you can set how they relate to each other. There are two types of constraints: union and intersection:

- **Union constraint** – This triggers an action when **any** of the individual constraints are met (like the OR command in programming). When multiple constraints exist, they are union by default, but can be changed to intersection when creating an association (see [step 8](#) in [Create an association](#) below, page 79).
- **Intersection constraint** – This triggers an action when **all** the individual constraints are met (like the AND command in programming).

All associations are added to the Association Matrix.

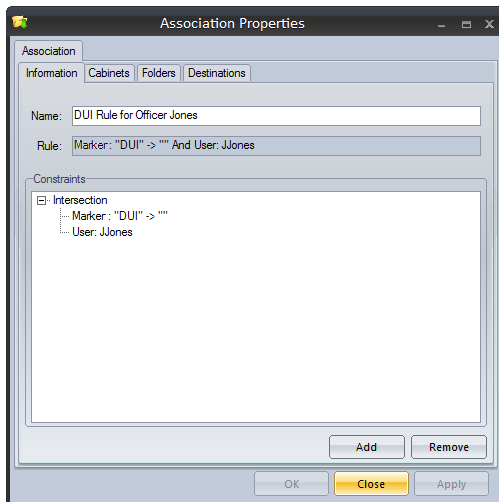
Association examples

These are examples of how associations appear in Evidence Local, based on real world situations.

Example A

An administrator wants to track all DUIs submitted by Officer Jones and place them in a specific location only accessible by him. Additionally, the DUI files should go to the normal file location. The administrator adds a [storage location](#) named *Secure San* and adds a folder named *Jones-DUI* with Access Control allowing only Officer Jones.

The administrator creates an intersection constraint that looks like this:



The **Rule** field summarizes the constraints below it as **Marker: "DUI" -> "" And User: JJones**. This means this association only triggers when user JJones uploads videos AND they have the DUI marker. On the **Folders** tab, the admin adds a *Jones-DUI* folder. When saved, this association appears in the association list:

Name	Constraints	Cabinets	Folders	Destinations
DUI Rule for Officer Jones	Marker : "DUI" -> "" And User: JJones	(none)	Jones-DUI	(none)

Files uploaded by JJones without the DUI tag will not be included in this association, nor will files tagged with DUI but uploaded by other officers.

Example B

Administrator Alvin wants to send all traffic stop files to a low-cost storage array and only keep them in Evidence Local for 90 days.

1. Alvin creates a [folder](#) named *Traffic Stops*, sets the retention to 90 days, and assigns the folder to the storage location *Low Cost SAN*.

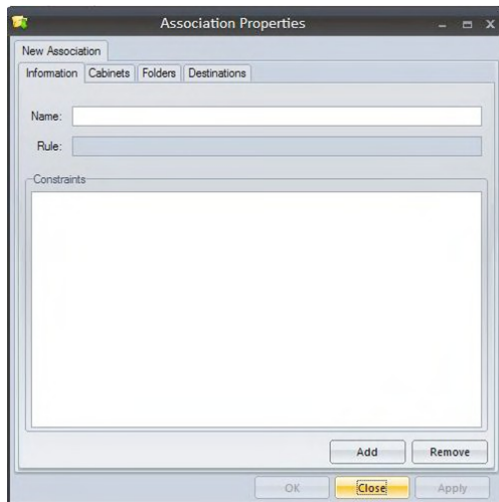
2. Alvin creates an association (next section) with the constraints marker event type *Traffic*, description keywords *Traffic*, and tag *Traffic*.
3. Alvin adds the folder *Traffic Stops*.

After Alvin saves, the association appears in the association list:

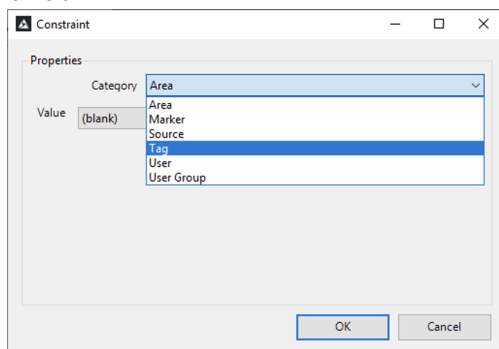
Name	Constraints	Cabinets	Folders	Destinations
Traffic Files Rule	Marker : "Traffic" -> "Traffic" Or Traffic: "Traffic"	(none)	Traffic Stops	(none)

Create an association

1. Select **Administration** from the [Quick menu](#) (page 3), then the **Associations** tab.
2. Select **Add** to show the **Association Properties** dialog box:



3. Enter a **Name** for the association.
4. Select **Add**.
5. Select the **Category** for the constraint. This defines what the association will check.



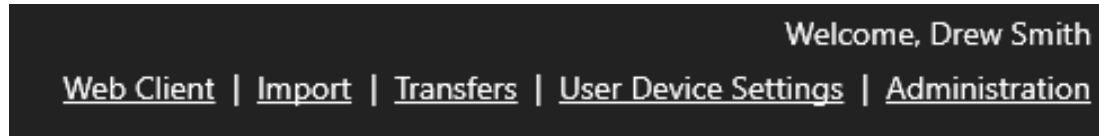
6. Enter or select the **Value** for the constraint. The available values depend on the category you selected:

- **Area** – Select from a list of areas.
 - **Marker** – Select the Event Type and enter a description as follows:
 - **Event Type** – Select from a list of event types. Or, enter a new type.
 - **Description** – In the text box, enter keywords to look for in a marker description.
 - **Source** – Select from a list of the sources.
 - **Tag** – Select from a list of tag templates. The tag template type, Choice or Text, appears before the name.
 - For a choice tag, make the appropriate choice for the association.
 - For a text tag, enter the value for the association.
 - **User** – Select from a list of users.
 - **User Group** – Select from a list of user-groups.
7. Select **OK** to add the constraint to the list and update the Rule field.
 8. Repeat steps 4–7 to add all the constraints for this association. If you add multiple constraints, set how they relate to one another: Union or Intersection (see [discussion](#) above on page 76).
 - To change a union constraint to intersection, right-click **Union** and select **Change to Intersection Constraint**.
 - To change an intersection constraint to union, right-click **Intersection** and select **Change to Union Constraint**.
 - To add another constraint, right-click **Union** or **Intersection**, select **Add > Atomic Constraint**, and follow steps 5–7.
 9. To send the file to a cabinet, select the **Cabinets** tab, select **Add**, and select the cabinet(s) to add.
 10. To send the file to a folder, select the **Folders** tab, select **Add**, and select the folder(s) to add.
 11. To send the file to a destination, select the **Destinations** tab, select **Add**, and select the destination(s) to add.
 - Optionally, assign a priority number to the destination. This determines the order in which assets are sent to other destination locations. The value can be any whole number from 1 to 999; the highest priority is 1.
 12. When finished with the association settings, select **Apply** to add the association.
 13. Select **Close** to exit.

Manage storage locations

This and all remaining sections in this manual are intended for Evidence Local administrators. For user-based topics, start at the [Overview](#) on page 1.

If this is in fact the 'droid you're looking for, select **Administration** from the Quick menu.



If you don't see a tab for **Locations** on the Administration page, your account requires additional rights.

Overview

Storage locations are represented by UNC (Universal Naming Convention) paths to locations on the network where files are physically stored that can be managed by Evidence Local.

The number of storage locations Evidence Local can manage is unlimited, but does depend on your license. This is a powerful tool for distributed storage of your files. Evidence Local incorporates storage locations into the Association Matrix as physical locations of the files grouped into logical folders. Evidence Local automatically manages when to delete files from these storage locations based on retention times set on the corresponding folders.

If you add a new location and switch folders to that location, Evidence Local will move all the data from the old location to the new, with managed and checked data migration from one location on the network to another.

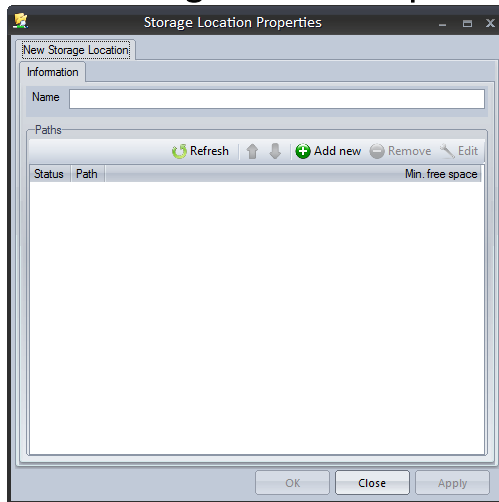
Evidence Local creates two default storage locations during installation:

- **Default storage location** – The UNC Path for this location is
\\[Evidence Local Server]\videos\Archive\
- **Offline storage location** – The UNC Path for this location is
\\[Evidence Local Server]\videos\Offline\

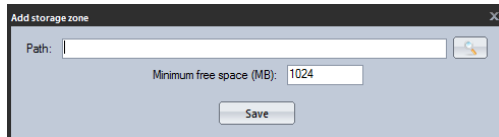
The default storage location is set up to store the initial Evidence Local archive. The offline storage location is the path to send files not recognized by Evidence Local, which includes files with a file extension not listed in the [File extension list](#) (page 95) and files with metadata issues.

Add a storage location

1. Select **Administration** from the [Quick menu](#) (page 3), then the **Locations** tab.
2. Select **Add**.
3. On the **Storage Location Properties** window, enter a **Name** for the location.



4. Select **Add new**.
5. Enter a **Path** or **Browse**  to a network location.



6. Enter the **Minimum free space** to leave on the storage location. Evidence Local stops using the storage location if the remaining space on the location is equal to or less than this setting.
7. **Save** the location to add the path to the list.
8. Repeat steps 4–7 to add all paths for the storage location. Normally a storage location only has a single path. However, in Evidence Local a storage location can be a pool of paths Evidence Local users to store files in order of preference. This allows Evidence Local a bit of elasticity for storage. You can add additional path to a storage location instead of creating a new one. This is great when you run out of space in one path or number of paths, but don't necessarily want to add hardware to expand those paths. In this case, you can find more space on your network and add that path to the list.
9. If you have multiple paths, set the priority by selecting a path in the list and selecting the arrow as needed. Evidence Local writes to the path at the top of the list first and works its way down.
10. Select **Apply** to save the storage location.
11. Select **Close** to exit.

Edit a storage location

1. Select **Administration** from the [Quick menu](#), then the **Locations** tab.
2. In the **Storage Locations** dialog box, use the filters to find the desired location.
3. Double-click the storage location row.
3. Edit the path information using the **Add**, **Edit**, or **Remove** options.
4. Select **Apply** to save the changes.
5. Select **Close** to exit.

Change storage location priority

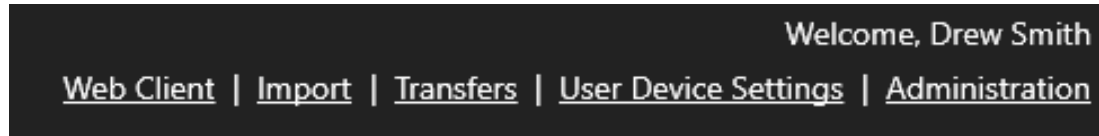
Storage locations have a priority. Evidence Local writes to storage location at the top of the list first, then works its way down.

1. Select **Administration** from the [Quick menu](#), then the **Locations** tab.
2. In the **Storage Locations** dialog box, use the filters to find the desired location.
3. Select the storage location row to change.
4. Use the **Up** and **Down** buttons at the bottom of the list to change the location's priority position.

Manage ingestion points

This and all remaining sections in this manual are intended for Evidence Local administrators. For user-based topics, start at the [Overview](#) on page 1.

If this is in fact the 'droid you're looking for, select **Administration** from the Quick menu.



If you don't see a tab for **Ingestions** on the Administration page, your account requires additional rights.

Overview

The default method for importing files to Evidence Local is through ingestion points. Evidence Local monitors all ingestion points in the system, periodically checking them for new files to ingest. Ingestion points are configured as either Standard or Hot.

Standard ingestion points process files using a standardized method and consider various proprietary metadata formats created by compatible third-party systems and a standard metadata format.

NOTE An SDK is available to third-party software developers who want to use Evidence Local automated standardized metadata Ingestion or add Evidence Local back-end management capability to their digital video, audio, or image recording solution. Contact your Axon representative for more details on integrating your media acquisition solution with Evidence Local.

During installation, Evidence Local creates a single standard ingestion point with the path

```
\\[Evidence Local Server]\videos\Ingestion\.
```

Hot ingestion points process files with user-specified metadata. File extensions must be set up in the file extensions matrix for them to be recognized by Evidence Local. Hot ingestion points allow administrators to set up folders monitored by Evidence Local that ingest all files placed into them and also assign pre-set metadata. Hot ingestion points are also an easy way to ingest large numbers of files without using the [import](#) tool (page 35).

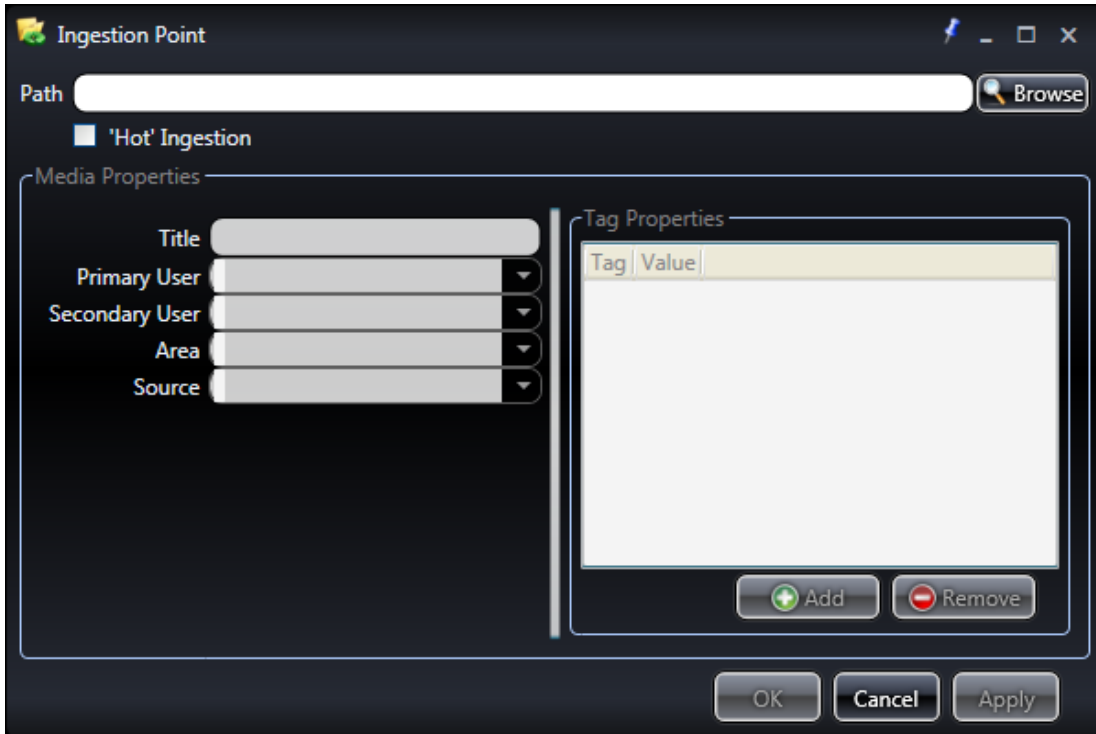
For example: to set up a hot ingestion point for all digital photos taken by a specific department, an administrator would:

1. Create a network folder.
2. Create a hot ingestion point with the directory's UNC path.

3. Set up metadata that adds a tag with the department's name to each file placed in the hot ingestion point.

Add an ingestion point

1. Select **Administration** from the [Quick menu](#) (page 3), then the **Ingestions** tab.
2. Select **Add**.
3. In the **Ingestion Point** dialog box, enter in a valid UNC Path or **Browse**  to find it.



4. To add a hot ingestion point:
 - a. Select the **'Hot' Ingestion** checkbox.
 - b. Enter the metadata information you want assigned to every file ingested from this point. This follows the same metadata available in the [import](#) tool (page 35).
 - c. In **Tag Properties**, select **Add** and select the tag information to add a tag to the file.
5. Select **Apply** to save the ingestion point.
6. Select **Close** to exit.

Change priority

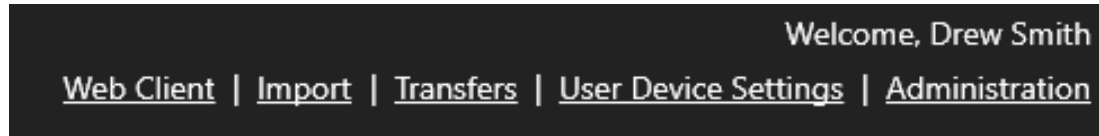
Ingestion points have priority like storage locations, with points at the top of the list being highest.

1. Select **Administration** from the [Quick menu](#), then the **Ingestions** tab.
2. In the **Ingestions** dialog box, use the filters to find the desired ingestion point.
3. Select the ingestion point row.
4. Use the **Up** and **Down** arrows at the bottom of the list to change the priority position of the ingestion point.

Manage destinations

This and all remaining sections in this manual are intended for Evidence Local administrators. For user-based topics, start at the [Overview](#) on page 1.

If this is in fact the 'droid you're looking for, select **Administration** from the Quick menu.



If you don't see a tab for **Destinations** on the Administration page, your account requires additional rights.

Overview

Use destinations to copy files to another Evidence Local server or folder. There are two types of destinations: server and folder.

Server destinations let administrators set up association rules that automatically copy files from one Evidence Local server to another when a rule criteria is met.

For example: The Evidence Local server at a Sheriff's Department needs to send DUI video files to the District Attorney (DA) office, which also has a Evidence Local server. They would:

1. Configure a server destination on the sheriff's Evidence Local to point to the DA's Evidence Local.
2. Create a rule to distribute video files with the tag DUI to the DA's Evidence Local.

Every file copied to a server destination triggers an automatic audit of the transfer, and the server destination can see which Evidence Local servers have sent files to it through the distribution feature.

Folder destinations let administrators set up association rules that automatically copy files to a specified folder when a rule criteria is met.

For example: An administrator wants to set up a process to automatic create offline DVD backups of all DUI videos instead of manually using the **Burn a DVD** operation. They would:

1. Create a folder destination to a network share.
2. Creae an association rule that copies video files with the DUI tag to the folder destination.

The administrator has a DVD software tool that checks the network share for files and automatically burns data DVDs.

Add a destination

1. Select **Administration** from the [Quick menu](#) (page 3), then the **Destination** tab.
2. Select **Add**.
3. In the **Destination Point** dialog box, enter the **Name** for the destination.

4. Select the **Remote Evidence Local server** or **Folder** radio button (if you see Commander, that's the former name of Evidence Local).
5. Add the destination **Value** information:
 - **Remote Evidence Local server** – Enter the IP Address or DNS name of the Evidence Local server.
 - **Folder** – Enter a valid UNC (Universal Naming Convention) path or local path.

NOTE Enter folder destinations from the server's perspective. A local value entered must be local to the server, not to the Evidence Local. For example, if the folder destination copies to a removable hard drive on a machine other than the server, use a UNC path. If it coies to a removable hard drive on the server, use a local path.

6. Select **Apply** to save the destination.
7. Select **Close** to exit.

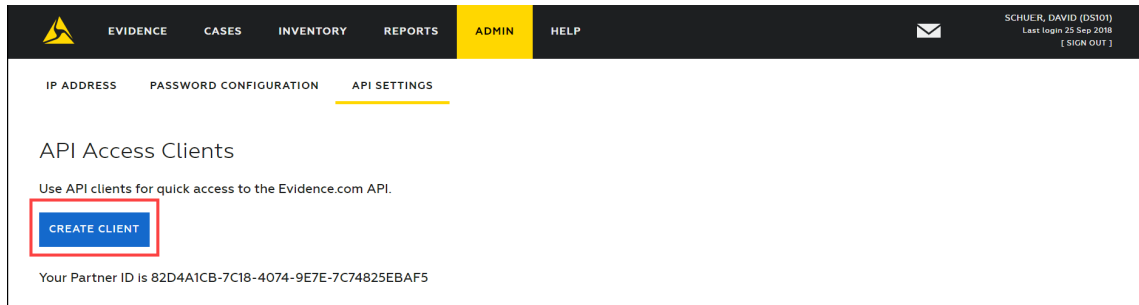
Add an Evidence.com destination

Prior to adding an Evidence.com destination, you must create an API Client through the Evidence.com interface.

1. Sign into the Evidence.com instance that will be the destination point.
2. On the menu bar, select **Admin > Security Settings > API Settings**. If you don't see API Settings on the page, it isn't enabled on the currently accessed instance. Use another instance or ask the Axon Technical Support team about activating this feature.



3. Select **Create Client**.



4. In **Client Description**, enter a meaningful name for the API client.

5. Set the following items to **Allowed**:

- EVIDENCE – any.create
- DEVICE – any.modify
- USERS – read

ADMIN

IP ADDRESS PASSWORD CONFIGURATION **API SETTINGS**

API Access Clients

Use API clients for quick access to the Evidence.com API.

Client Description:

USHER

▶ open_websocket	☐ ALLOWED	☒ PROHIBITED
------------------	-------------------------------	---

EVIDENCE

▶ any.create	☐ ALLOWED	☒ PROHIBITED
▶ any.read	☐ ALLOWED	☒ PROHIBITED
▶ any.audit	☐ ALLOWED	☒ PROHIBITED
▶ any.modify	☐ ALLOWED	☒ PROHIBITED
▶ any.share	☐ ALLOWED	☒ PROHIBITED
▶ sharewith	☐ ALLOWED	☒ PROHIBITED
▶ any.cewLog	☐ ALLOWED	☒ PROHIBITED

TRANSCRIPTION

▶ accounts.modify	☐ ALLOWED	☒ PROHIBITED
▶ orders.create	☐ ALLOWED	☒ PROHIBITED

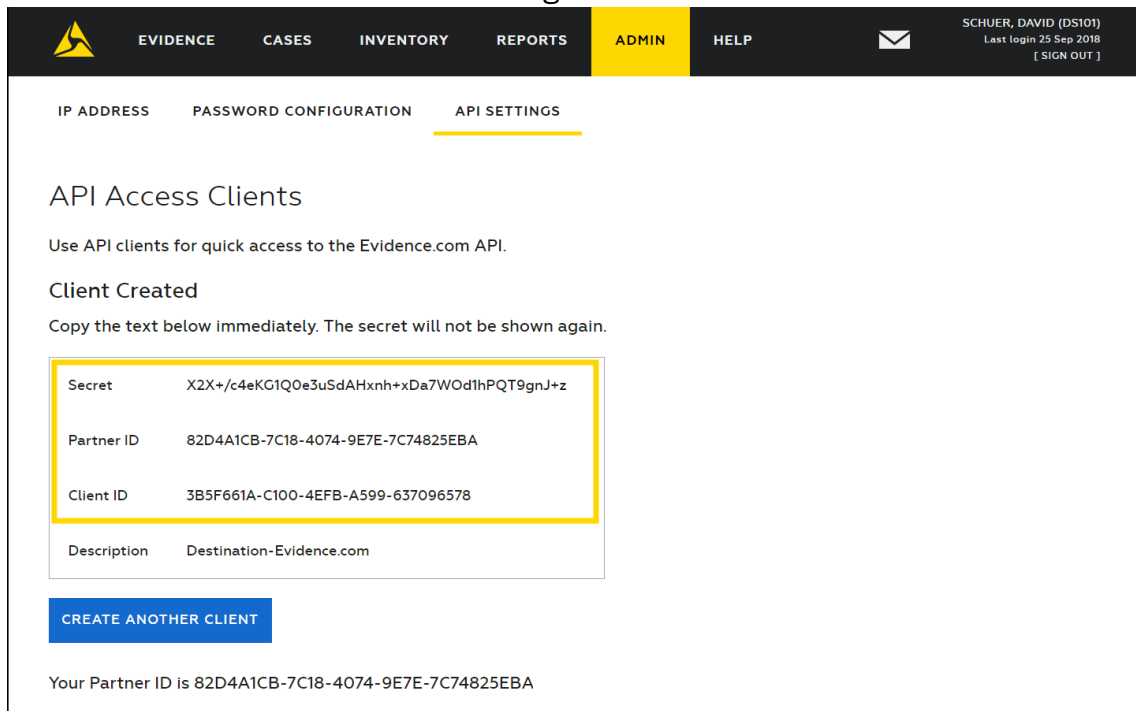
DEVICE

▶ any.modify	☐ ALLOWED	☒ PROHIBITED
--------------	-------------------------------	---

6. Select **Save**. Evidence.com saves the client and displays the secret, the partner ID, the client ID, and the client description.

NOTE This is the only time you can see the client secret. As soon as you leave the page or select Create Another Client, the secret becomes inaccessible.

7. Record the Secret, Partner ID, and Client ID. You will enter this information in the Evidence Local **Destination Point** dialog box.

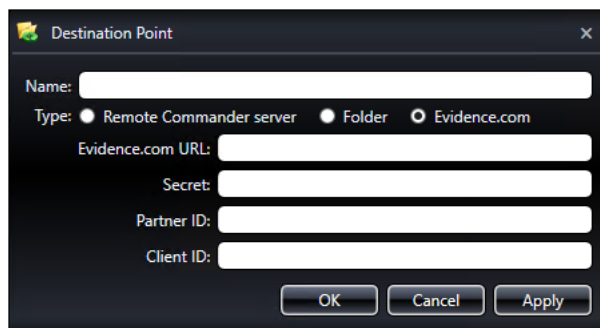


The screenshot shows the Evidence Local Admin interface. The top navigation bar includes tabs for EVIDENCE, CASES, INVENTORY, REPORTS, ADMIN (highlighted), and HELP. The user is identified as SCHUER, DAVID (DS101) with a last login on 25 Sep 2018. The ADMIN section has sub-tabs for IP ADDRESS, PASSWORD CONFIGURATION, and API SETTINGS (highlighted). The main content area is titled "API Access Clients" and includes instructions to use API clients for quick access to the Evidence.com API. A section titled "Client Created" provides a warning to copy the text immediately as the secret will not be shown again. Below this, a table displays the generated credentials:

Secret	X2X+/c4eKG1Q0e3uSdAHxnh+xDa7Wod1hPQT9gnJ+z
Partner ID	82D4A1CB-7C18-4074-9E7E-7C74825EBA
Client ID	3B5F661A-C100-4EFB-A599-637096578
Description	Destination-Evidence.com

Below the table is a blue button labeled "CREATE ANOTHER CLIENT". At the bottom, a message states: "Your Partner ID is 82D4A1CB-7C18-4074-9E7E-7C74825EBA".

8. Open Evidence Local for the instance you want to connect to Evidence.com.
9. Select **Administration** from the [Quick menu](#), then the **Destinations** tab.
10. Select **Add**.
11. In the **Destination Point** dialog box, select the **Evidence.com** radio button.



The screenshot shows the "Destination Point" dialog box. It has a title bar with a close button. The "Name:" field is empty. The "Type:" section has three radio buttons: "Remote Commander server", "Folder", and "Evidence.com" (which is selected). Below the radio buttons are four text input fields: "Evidence.com URL:", "Secret:", "Partner ID:", and "Client ID:". At the bottom are three buttons: "OK", "Cancel", and "Apply".

12. Enter the **Name** for the destination, enter the URL for the [Evidence.com](#) instance (such as <https://www.Evidence Local.evidence.com>).
13. Enter the **Secret**, **Partner ID**, and **Client ID** from step 7.
14. Select **Apply** to save the destination.
15. Select **Close** to exit.

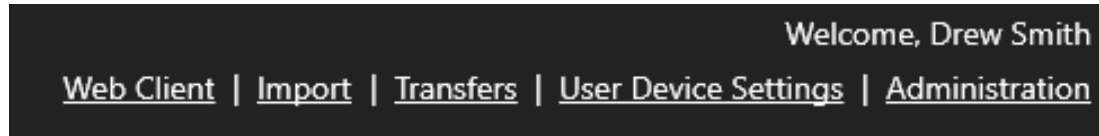
Edit a destination

1. Select **Administration** from the [Quick menu](#), then the **Destination** tab.
2. In the **Destination** dialog box, use the filters to find the desired ingestion point.
3. Double-click on the destination row.
4. Edit the destination information as needed.
5. Select **Apply** to save the changes.
6. Select **Close** to exit.

Reports

This and all remaining sections in this manual are intended for Evidence Local administrators. For user-based topics, start at the [Overview](#) on page 1.

If this is in fact the 'droid you're looking for, select **Administration** from the Quick menu.



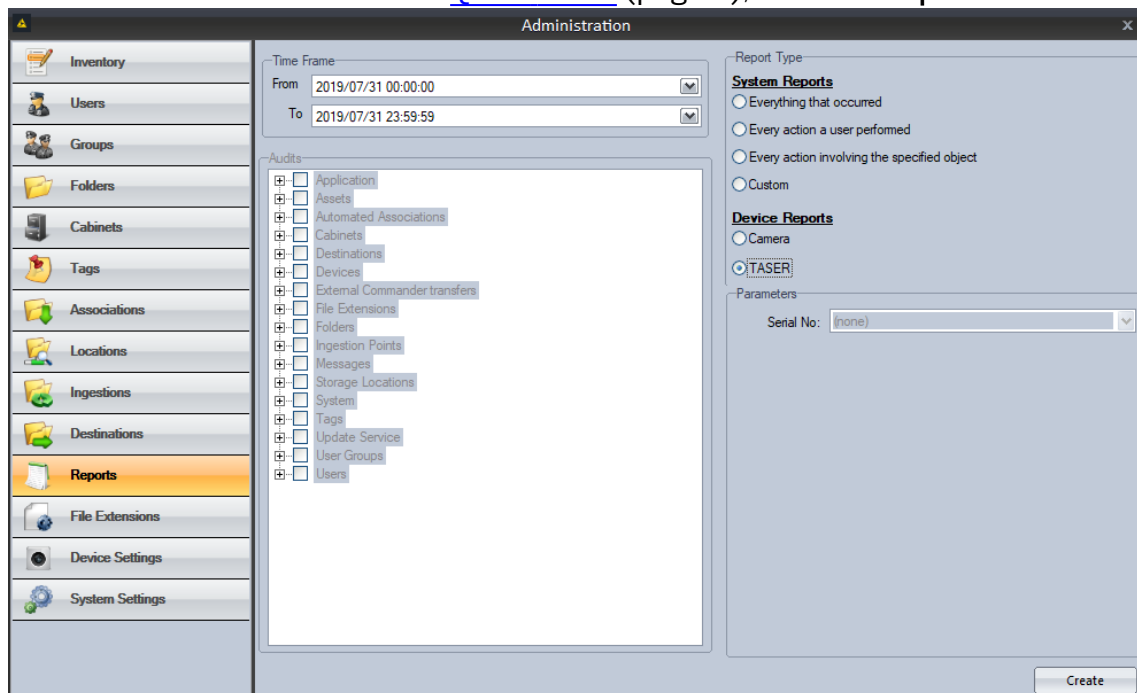
If you don't see a tab for **Reports** on the Administration page, your account requires additional rights.

Overview

Administrators and users with the **Create Reports on users and system activity** right can run detailed reports on Evidence Local operations.

System report

1. Select **Administration** from the [Quick menu](#) (page 3), then the **Reports** tab.



2. Select the Time Frame **From** and **To** date and time for the report period.

3. Select the **Report Type**:

- **Everything that occurred** – Reports everything that happened in Evidence Local within the specified time-frame.
- **Every action a user performed** – Reports everything that happened for a specific user within the specified time-frame.
- **Every action involving the specified object** – Reports everything that happened to a specified object (cabinet, folder, location, tag, user, or user group) within the specified time-frame.
- **Custom** – Reports on the selected user (optional) and up to two objects (optional).

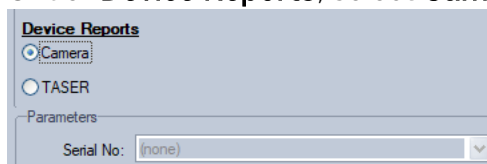
NOTE A red parameter value means that object was deleted from Evidence Local. However, an audit trail of that object still exists. This is useful if destructive behavior was attempted; a report can highlight this.

4. Select any needed parameters, based on the report type selected. If you are using the **Only include assets listed in search results** parameter, search in the Evidence Local client before running the report.
5. Adjust the audits for the report as needed. The audits list is available to edit for **Every action involving a specified object** or **Custom** report types. There are 15 different audit sections and 133 different audit actions to select for or exclude from a report.
6. Select **Create**.

The report is generated and displayed in a report viewer window. A complex report will take more time to generate than a simple one.

Camera report

1. Select **Administration** from the [Quick menu](#) (page 3), then the **Reports** tab.
2. Select the Time Frame **From** and **To** date and time for the report period.
3. Under **Device Reports**, select **Camera**.



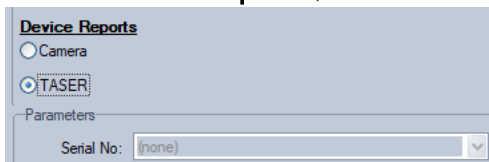
The screenshot shows a web interface titled "Device Reports". Under this title, there are two radio button options: "Camera" (which is selected) and "TASER". Below these options is a section labeled "Parameters". Inside the "Parameters" section, there is a label "Serial No:" followed by a dropdown menu that currently displays the word "none".

4. Enter the **Serial number** of the camera.
5. Select **Create**.

When complete, the report will display in a report viewer window. A complex report will take more time to generate than a simple one.

TASER report

1. Select **Administration** from the [Quick menu](#) (page 3), then the **Reports** tab.
2. Select the Time Frame **From** and **To** date and time for the report period.
3. Under **Device Reports**, select **TASER**.

The screenshot shows a web interface titled "Device Reports". It has two radio buttons: "Camera" and "TASER". The "TASER" radio button is selected and highlighted with a dashed border. Below the radio buttons is a section labeled "Parameters". Inside this section, there is a label "Serial No:" followed by a dropdown menu that currently displays "(none)".

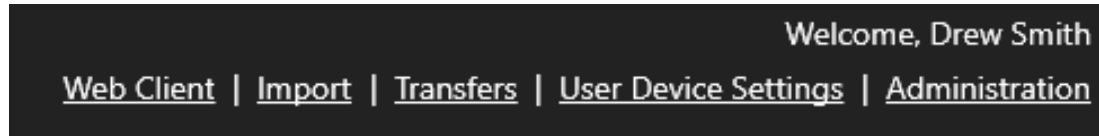
4. Enter the serial number of the TASER handle.
5. Select **Create**.

When complete, the report will display in a report viewer window. A complex report will take more time to generate than a simple one.

Manage file extensions

This and all remaining sections in this manual are intended for Evidence Local administrators. For user-based topics, start at the [Overview](#) on page 1.

If this is in fact the 'droid you're looking for, select **Administration** from the Quick menu.



If you don't see a tab for **File extensions** on the Administration page, your account requires additional rights.

Overview

Evidence Local uses a file extensions list to understand the files it ingests. This list can be expanded to any extension needed and Evidence Local performs the necessary tests behind the scenes to validate what can be done with the file.

By default, Evidence Local supports the following extensions: 3GP, ASF, AV, AVI, BMP, G64, GIF, JPEG, JPG, MKV, MOV, MP3, MP4, MPEG, MPG, PEF, PNG, SMD, TIF, TIFF, WAV, WMA, WMV, and ZIP.

Add a file extension

1. Select **Administration** from the [Quick menu](#) (page 3), then the **File Extensions** tab.
2. Select **Add**.

3. On the **File Extension Properties** dialog box, enter the **Brand Type** for the extension, if known.

The screenshot shows the 'File Extension Properties' dialog box with the 'New File Extension' tab selected. The 'Information' section contains the following fields and controls:

- Extension:** A text input field.
- Brand Type:** A text input field.
- Description:** A text input field.
- File Type:** A dropdown menu with a downward arrow.
- Open With:** A dropdown menu currently showing 'Auto-select'.
- Thumbnails:** A dropdown menu currently showing 'Auto-select'.
- Command:** A text input field.
- Arguments:** A text input field.
- Check file:** A button located to the right of the 'File Type' dropdown.

The 'Options' section contains the following checkboxes:

- ☐ Show thumbnails
- ☐ Enable import
- ☐ Commander player support
- ☐ Standalone player direct playback
- ☐ Allow conversion to standard media
- ☐ Allow burn to authored DVD
- ☐ Allow direct access from external program

At the bottom of the dialog are three buttons: 'OK', 'Close', and 'Apply'.

4. Enter a **Description** for the extension.
5. Select the extension **File Type**.
6. To test a sample file with the extension you want to add:
 - b. Select **Check file**.
 - c. Enter the path to the sample file or select **Browse ...** to find it.
 - d. Select **Check File**. Evidence Local opens and inspects the file to ensure it can be successfully opened and played.
6. Select **Open With** and assign an application for the extension.
7. If this extension supports thumbnails, set **Thumbnails** to **Display**.
8. Add the **Command**.
9. Add any **Arguments**.
10. Select **Options**:
 - **Show thumbnails** – Evidence Local player will generate thumbnails if it can play this type of file.

- **Enable import** – Allow the Import tool to see files with this extension during the import search.
- **Evidence Local player support** – Allow a file to be viewed and played in the player integrated into the Evidence Local client.
- **Standalone player direct playback** – Allow a file to be viewed and played in the external standalone player that is optionally included on video export.
- **Allow conversion to standard media** – Allow conversion of video files to standard media format. This option is only available for video file extensions that can be played with the Evidence Local player.
- **Allow burn to authored DVD** – Allow files with this extension to be burned to an authored DVD. This option is only available for video file extensions that can be played with the Evidence Local player.
- **Allow direct access from external program** – Enable a direct opening of a file from its storage location. This directly modifies the file at the storage location with the program that is opening the file. The file is out of Evidence Local control at this point. However, there is an audit trail showing this action and if the file's MD5 hash is changed. If this option is not selected, Evidence Local copies the file to the local client workstation for opening with the non-Evidence Local application.

11. Select **Apply**.
12. Select **OK** and **Close** to exit.

The new file extension appears in the list.

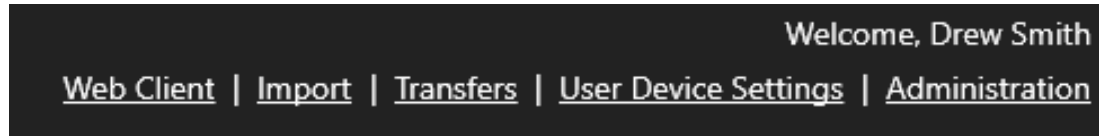
Edit a file extension

1. Select **Administration** from the [Quick menu](#), then the **File Extensions** tab.
2. In the **File Extensions** dialog box, use the filters to find the desired extension.
3. Double-click the file extension row.
4. In the **File Extensions Properties** dialog box, edit the information as needed.
5. Select **Apply** to save the changes.
6. Select **Close** to exit.

Manage device settings

This and all remaining sections in this manual are intended for Evidence Local administrators. For user-based topics, start at the [Overview](#) on page 1.

If this is in fact the 'droid you're looking for, select **Administration** from the Quick menu.



If you don't see a tab for **Device settings** on the Administration page, your account requires additional rights.

Overview

Administrators and users with the **Manage device configuration** right can define agency-wide settings for Axon body-worn cameras, Axon Fleet cameras, Axon Signal vehicle devices, and TASER devices.

Body-worn camera (BWC) settings

Use the **BWC Settings** tab to define settings for Axon cameras, such as Axon body and Axon Flex. Settings include video quality, event pre-buffering, audio mute control, indicator light control, and others.

NOTE Some setting changes can only be enforced after the camera has been inserted in an Axon Dock or connected to an Evidence Sync application.

Selecting a label shows a description of the setting. Settings are also described later in this section.

Use microphone controls if your agency restricts audio recordings.

Video quality settings let you define the video encoding rate or the space used per hour of recording. This is useful for agencies needing to manage network bandwidth usage. To ensure video quality remains acceptable, always validate the effect of changes to camera video quality.

Change settings

1. Select **Administration** from the [Quick menu](#) (page 3), then the **Device Settings** tab.
2. Select the **BWC Settings** tab.

3. Select the body-worn camera type, such as **Axon Body 4** or **Axon Body & Flex**.
4. For each setting, choose the option that best supports your agency's policies regarding video, audio, and offline camera usage. Options are generally self-descriptive, but to see them all described in one place, refer to the following section.
5. To reset to default values, select **Defaults**.
5. Select **Apply** to save changes.

Body camera setting descriptions

Not all settings listed here are available for all cameras. Systems are abbreviated as:

- AB3 – Axon Body Camera 3
- AB2 – Axon Body Camera 2
- AB1 – Axon Body Camera
- AF2 – Axon Flex Camera 2

Video

- **Quality** – Set the video quality of recordings. Higher quality videos will take up more storage space. For a good balance of quality and storage space, Axon recommends using 720p High (the default).
 - AF1: use Medium.
- **Pre-event buffer** – Pre-event video buffer will be included in a video. The buffer time is configurable in 30-second increments for up to two minutes. When enabled, video from the selected amount of time prior to the user starting a camera recording is included in the final video. Default: 30 seconds.
 - AB2/AF2: buffers above 30 seconds requires v1.9 firmware or higher. A two-minute buffer is unavailable with a quality of High HD (1080P).
 - AB1: 30 seconds only.
- **Watermark** – Sets a permanent watermark with date, time, and camera serial number in the upper right corner of videos. The watermark time uses the ISO 8601 international standard 24-hour format with a trailing Z for "Zulu" or "zero hours" from Coordinated Universal Time (UTC) time standard. Default: Enabled.
- **Watermark local time zone** – Determines the time zone displayed in the permanent watermark. When enabled, uses the local time zone, based on agency configuration. When disabled, uses UTC. Default: enabled.
- **Video Recording Indicator (AB2/AF2)** – Provides a visible indication of recording status on the front of the camera using the battery LED. Stealth mode must be disabled for this setting to be enabled.

- **User Control of Stealth and Indicator modes (AB2/AF2)** – Lets camera users toggle Stealth mode or indicator lights. AB2 and Flex 2 cameras emit lights, sounds, and haptic feedback (vibrations) when they are switched on or off and when a user starts or stops recording. In Stealth mode, all lights, sounds, and vibrations are turned off. When users disable indicator lights, all lights are turned off. These settings will also disable the front camera light regardless of the **Video Recording Indicator** setting.

Audio

- **Audio recording**– Records audio along with video. If **Users can mute during recording** is enabled, users can toggle audio recording for their camera. Default: enabled.
 - AB2/AF2: To disable audio, select **Disable Camera Audio**. To prevent users from turning audio recording back on, set **User Control of Audio Recording to Prohibit Users from Toggling Camera Audio**.
- **Pre-event buffer** – Includes audio in the pre-event buffer. Default: disabled.
- **User Control of Audio Recording (AB2)** – Lets users toggle audio while recording an event by pressing the function button for three seconds.

Lights (AB3)

- **Front light** – Enables the visible indication of the recording status on the front triad LEDs. During pre-event buffering, the LEDs blink green. During recording the LEDs blink red. Stealth Mode must be disabled for this setting to be enabled. Default: disabled.
 - AB2: uses the battery light.
- **Automatic Brightness** – Enables LED Auto Brightness mode, which automatically adjusts the brightness of front and top LED lights based on ambient light. If front lights are disabled, the changes only apply to top light. Users must have permission to adjust indicator lights to enable Auto mode from the camera or Axon applications. Stealth mode must be disabled for this setting to be enabled. Default: disabled.

Location (AB3)

- **Record location in video** – Embeds GPS data in videos. Default: enabled.
- **Location information available to Axon Respond** – Makes location information available in near real-time to authorized agency users. Requires Axon Respond. Default: Location available when camera is recording. If **Location available when camera is recording and buffering** is selected, camera location is reported to Axon Respond while the camera is recording or buffering. Camera location while the camera is buffering is updated the Respond platforms every 15 minutes and

denoted on the map as device markers. Camera location while recording is updated every few seconds.

IMPORTANT With **Location available when camera is recording and buffering** enabled, users can expect a 5–10 minute reduction in total camera run-time.

Signal (AB3)

- **Signal** – If enabled, camera will begin recording per Axon Signal instruction. If disabled, they will not. Set trigger events in [Axon Signal settings](#) (page 105). Default: disabled.

Streaming (AB3)

- **Livestreaming** – Cameras can stream audio and video to authorized agency users while recording. Requires Axon Respond+. Default: enabled.

Activity detection (AB3)

- **Gunshot detection recording** – Cameras starts recording when sensors detect the camera wearer discharged a firearm. Default: disabled.
- **Gunshot detection notification** – Notifies authorized agency users in near real-time. Requires Axon Respond. Default: disabled.

App support (AB3)

- **Axon View pairing** – Cameras can pair with Axon View. Default: enabled.
- **Video playback from device** – Users can play video while it is still on the camera using Axon View or Axon View XL. Default: enabled.

Evidence upload (AB3)

- **Throttle camera upload speed** – Cameras upload speed is throttled when docked. When enabled, enter the maximum MB/second limit per camera. Default: disabled.

User permissions (AB3)

- **Users can mute during recording** – Users can mute audio while recording using an on-camera button. Default: enabled.
- **Users can adjust indicator light settings** – Users can toggle their camera indicator lights using an on-camera button, or with Axon View, Axon View XL, and Evidence Local. Default: enabled.

- **Users can adjust vibration settings** – Users can toggle vibration (haptic) settings of their camera with Axon View, Axon View XL, and Evidence Local. Default: enabled.
- **Users can use stealth mode** – Users can toggle Stealth mode on their camera using an on-camera button, or with Axon View, Axon View XL, and Evidence Local. Default: enabled.
- **Users can use sleep mode** – Users can toggle Sleep mode on their camera. Sleep mode is an idle state that disables recording and buffering. Its an alternative to powering off the camera, allowing transition back to buffering in less than four seconds. Default: enabled.

Axon View

- **Mobile Device Pairing** – Toggles a camera's ability to pair with the Axon View mobile app. Enabling to turn on Bluetooth Low Energy (BLE) Peripheral mode and Wi-Fi.
- **Mobile Device Playback** – Lets users play body camera recordings within the Axon View application. When disabled, users can't preview their body camera video, regardless of the camera assigned to them.

Global settings

- **Allow Users to Modify Device Name** – Lets users modify the **Device Name** of cameras assigned to them in the [User device settings](#) dialog box. Otherwise, only administrators can set the device name from the **All Devices** tab.
- **Enable Offline Mode for All Cameras (AB2/AB1/AF2/AF1)** – Allows individual devices to be set to standalone (offline) mode.

WARNING Enabling offline mode requires users to accept a disclaimer acknowledging risks to the agency and data when using offline mode.

Fleet settings

Use Fleet settings to define default settings for Axon Fleet system cameras, such as video quality, video pre-event buffering, audio mute control, and indicator light control.

Selecting a label shows a description of the setting. Settings are also described later in this section.

NOTE Some setting changes can only be enforced on a Fleet camera after its is updated by Axon View XL, inserted in an Axon Dock, or connected to an Evidence Sync application.

Video quality settings let you define the video encoding rate or the space used per hour of recording. This is useful for agencies needing to manage network bandwidth usage. To ensure video quality remains acceptable, always validate the effect of changes to camera video quality.

Change settings

1. Select **Administration** from the [Quick menu](#), then the **Device Settings** tab.
2. Select the **Fleet Settings** tab.

The screenshot displays the 'Fleet Settings' configuration window. It features a tabbed interface with 'Body Camera Settings', 'Fleet Settings', and 'Signal Configuration'. The 'Fleet Settings' tab is active, showing several configuration sections:

- Video Settings:** Includes settings for Pre-Event Buffering (Enable), Recording Indicator for Front and Rear Cameras (Enable for Buffering and Recording), Recording Quality for Front and Rear Cameras (Low HD (720P) - Recommended), User Control of Stealth and Indicators (Allow Users to Toggle Modes), and Watermark (Enable).
- Audio Settings:** Includes Audio Recording (Enable), User Control of Audio Recording (Allow Users to Toggle Modes), and Pre-Event Audio Buffering (Enable).
- Activation Settings:** Includes Speed Activation (checkbox), Value (MPH or KPH by the setting provided) (25-200), and Motion Activation (Enable).
- Offload Settings:** Includes Auto Offload Timer (6 Hours (Default)).

At the bottom of the window, there are 'Apply' and 'Defaults' buttons.

3. For each setting, choose the option that best supports your agency's policies regarding Fleet camera usage. Options are generally self-descriptive, but to see them all described in one place, refer to the following section.
4. To reset to default values, select **Defaults**.
5. Select **Apply** to save changes.

When View XL is connected to Evidence Local, it automatically checks for and applies any updated Axon Fleet settings every 10 minutes.

Fleet setting descriptions

Video settings

- **Pre-Event Buffering** – Video will be recorded in the pre-event buffer.
- **Show recording status with front camera light** – Enables the visible indication of the recording status on the Fleet camera. The light will blink green during pre-event buffering and red during recording.
- **Quality settings** – Each camera can have a different record quality setting. Higher quality videos will take up more storage space. For a good balance of quality and storage space, Axon recommends recording in low HD.
- **User Configurable Modes - Stealth and Indicator Lights** – Lets Fleet users toggle stealth mode or indicator lights on/off. Axon Fleet cameras emit lights and sounds when they are switched on or off, and when a user starts or stops recording. When officers enable stealth mode, all lights and sounds are turned off. Officers can change the brightness or turn off the LED indicator light on the front of the camera.
- **Watermark** – Sets a permanent watermark with date, time, and camera serial number in the upper right corner of videos. The watermark time uses the ISO 8601 international standard 24-hour format with a trailing Z for "Zulu" or "zero hours" from Coordinated Universal Time (UTC) time standard.

Audio settings

- **Camera Audio Recording** – Sets front and back cameras to include audio with video. Select **Disable** to not record audio.
- **Toggle Camera Audio Recording**– When allowed, lets users use View XL to toggle audio while the camera is recording. Only applicable if **Camera Audio Recording** (above) is enabled. When prohibited, users' can't toggle audio.
- **Pre-event buffering audio recording** – Includes audio in the pre-event buffer.

Activation settings

- **Speed Activation** – Set your Axon Fleet Front camera to transition from Buffering to Event mode to record video when the set speed threshold is exceeded. Select the Speed Activation check box and enter a value from 25–200. The units used, MPH or KPH, is determined by the [Interface configuration setting](#) (page 111). Default: off.

Important You must have a GPS-enabled router and the GPS must be configured for use with Axon Fleet for the Speed Activation setting to function.

- **Motion Activation** – Transitions Fleet cameras from Buffering to Event mode when sensors detect very high sudden changes in acceleration, usually associated with vehicle accidents or crashes. Default: disabled.

Offload Settings

- **Auto Offload Timer** – The duration evidence is stored in View XL before being automatically queued for upload to Evidence.com, from immediate to a delay of up to 12 hours, set in one-hour increments.

Axon Signal settings

Axon Signal is a technology that alerts your body, flex, or fleet camera to begin recording. With Axon Signal sending the alerts, officers can focus on critical situations instead of their cameras.

While Axon Signal Vehicle inputs and events are set on agency-wide basis, an Axon Signal Vehicle event for a vehicle will not alert the Fleet cameras for another vehicle. However, body worn cameras are alerted by events from any Axon Signal Vehicle.

For example, say an Axon Signal Vehicle is configured to alert body worn cameras and the Fleet front camera when the vehicle's light bar is turned on; when the vehicle's light bar turns on, the Fleet front camera and also any body-worn cameras within range are alerted to begin recording, but front cameras in other vehicles are not.

Set Signal triggers

1. Select **Administration** from the [Quick menu](#), then the **Device Settings** tab.
2. Select the **Signal Configuration** tab, then **Signal Vehicle**.

Signal Vehicle

These settings determine which 12V inputs activate Body Worn, Fleet 1, and Fleet 2 cameras.

INPUT	LABEL	RULE	CAMERAS
 5	-	-	- 
 6	-	-	- 
 7	-	-	- 
 8	-	-	- 
 9 [†]	-	-	- 
 10 [‡]	-	-	- 
 11 [‡]	-	-	- 
 12 [‡]	-	-	- 

[†] Signal Vehicle inputs 9, 10, 11, & 12 support activation delays and inputs 11 & 12 are best to use for lightbars. Signal Vehicle unit and Body Cameras require supporting firmware. Fleet 1 & 2 cameras do not support delays. See the Axon product guides on Signal Configuration for more information.
[‡] Inputs that are configured to Delay Activation will only delay on the first trigger event during a session. See the Axon product guides on Signal Configuration for more information.

Body Camera 12 V Signal Reactivation Sensitivity

Determines how sensitive Body Cameras are to repeated activation from the same vehicle based Signal device. This feature requires updated Camera and Signal Vehicle firmware. Specific firmware versions and a detailed explanation of behavior is available in the Fleet 3 User Manual.

☒ Cameras are less sensitive to reactivation. This is the default and legacy behavior. Cameras activate once per session.

☐ Cameras are more sensitive to reactivation. Cameras activate whenever an input is triggered.

The table shows how inputs configured for Axon Signal Vehicle in your agency. Inputs 1–4 are reserved and cannot be configured.

3. Select a Signal input row, then select the appropriate input from the drop-down list.
4. For each input that you want to alert body-worn, Fleet front, and Fleet rear cameras, select the corresponding check box.
5. Select **Apply**.

Optionally, select **Defaults** to clear all input information.

Respond settings

Respond settings include access to export the audit log, notification configuration options, and the warning configuration.

1. Select **Administration** from the [Quick menu](#), then the **Device Settings** tab.
2. Select the **Respond Settings** tab.

Respond Settings

Export audit log for Respond
Export agency wide Respond audit log in csv or pdf format.

Select File Type
☐ CSV ☒ PDF

Date Range All-time

Export Audit Log

Respond Notification Configuration

High Priority Alerts ⓘ

General Officer Activity ⓘ

Off ⓘ

CEW Armed ▼

CEW Trigger ▼

CEW Arc ▼

Gunshot ▼

Weapon Drawn ▼

Respond Warning Configuration
Determines if a warning message is displayed to users when accessing Respond features.

Enabled ☐

Warning Title * Beware of this feature

Warning Text * This is a sensitive information. Be aware!

Defaults

Save Cancel

3. **Export the audit log**, configure **Respond notifications**, or configure **Respond warning** as needed (details follow).
4. Select **Save** to save changes.

Export audit log for Respond

The agency audit log consolidates all Respond information, such as which users accessed the Respond map, into a single audit log. Only users with the **Respond view audit log** Right can export the audit log.

Audit trails will continue to show Respond information for individual devices and users.

1. Select the **Date Range** to be shown in the audit log.
2. Select the export **File type**.
3. Select **Export Audit Log** and select where to save the log.

Respond notification configuration

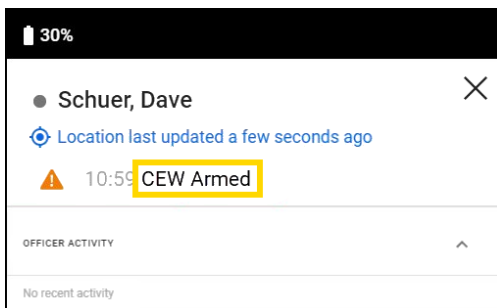
This section lets you configure which Axon Signal alerts are shown in Respond. It lists the activations you have available, based on Signal Configuration settings and Axon Body gunshot detection gunshot detection is in beta as of this writing).

Note –The Axon Body 3 gunshot detection feature is currently in beta testing.

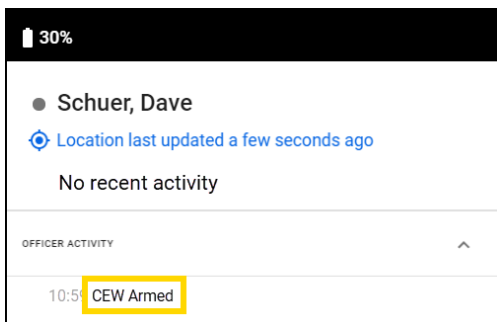
Each dropdown menu has three options:

- **High Priority Alerts** – When this notification occurs, an alert appears in the alerts banner on the Respond map, the associated camera marker is surrounded by a red circle, and the alert is added to the device marker.

High Priority Alerts
General Officer Activity
Off



- **General Officer Activity** – The information is only noted in the Officer Activity section on the device marker and will not generate an alert.



- **Off** – No information appears in Respond.

After changing activation settings, select **Save**.

Respond warning configuration

This allow wide access to the Respond map to remind users about the potentially sensitive information available on the map. When enabled, a custom warning message displays to users and must be confirmed before they can use the Respond map.

1. Select the **Enabled** checkbox. If clearing this checkbox, skip to step 4.
2. Enter the warning title and text:
 - a. **Warning Title** – Enter a title up to 25 characters long.
 - b. **Warning Text** – Enter the text for the message up to 255 characters long.
3. Select **Save**.

TASER 7 settings

This tab lets you configure TASER 7 to meet your agency policy.

1. Select **Administration** from the [Quick menu](#), then the **Device Settings** tab.
2. Select the **TASER Settings** tab.
3. Configure the settings (described below) to meet your agency policy.
4. Optionally, select **Defaults** to reset all settings to default values.
5. Select **Apply** to save the changes.

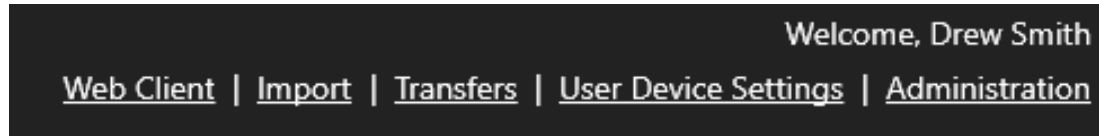
TASER 7 setting descriptions

- **Laser** – TASER 7 uses two lasers to identify approximate impact location of the top and bottom probes. This setting determines if the lasers are on steady or blinking.
- **Flashlight Power** – Sets the brightness of the TASER 7 flashlight.
- **Automatic Shut-Down** – Select from:
 - **Hard Stop** – The TASER stops electrical discharge after five seconds, regardless if the trigger or arc switch is being held.
 - **Arc Switch Override** – The TASER continues electrical discharge after five seconds if the arc switch is being held.
 - **Disabled** – The TASER continues electrical discharge after five seconds if the trigger and/or arc switch is being held.
- **Tilt Select** – Lets users switch the bay that will deploy when the trigger is pulled by using a quick sideways tilt of the device. The active cartridge will be underlined on the device display.
 - If both Close-Quarters and Stand-Off cartridges are loaded, the lasers will change to represent the angle of the active cartridge.
 - **Enabled – Training Only** – Available with Inert or HALT cartridges so users can test a feature prior to using live cartridges in the field.

Manage system settings

This and all remaining sections in this manual are intended for Evidence Local administrators. For user-based topics, start at the [Overview](#) on page 1.

If this is in fact the 'droid you're looking for, select **Administration** from the Quick menu.



If you don't see a tab for **System settings** on the Administration page, your account requires additional rights.

Overview

Use this tab for adjusting system-wide settings.

Standard system settings

The **Standard** tab has settings for retention of audit and activity logs, user password requirements, and other miscellaneous settings for Evidence Local.

Reach these settings by selecting **Administration** from the [Quick menu](#) (page 3), then the **System Settings** tab.

After changing standard settings, remember to **Save**.

Retention settings

On the **Standard** tab, select retention settings:

- **Retention of audit log (in days)** – How many days the audit log is retained.
- **Retention of Activity/Error Log** – How many days the activity log is retained.
- **Retention of audit and engineering log files** – How many days audit and engineering logs are retained.
- **Retention of TASER logs** – How many days TASER logs are retained.
- **Retention start date:**
 - **Folder/cabinet added date** – How many days evidence is retained from the date it is added to the folder/cabinet. It will be reset when evidence is moved to a new folder/cabinet.

- **Recorded date** – How many days evidence is retained from the date it is recorded.
- **Ingestion date** – How many days evidence is retained from the date the evidence is ingested into the system.

Password settings

On the **Standard** tab, select user password settings. These settings do not affect Active Directory users.

- **Minimum password length** – The minimum number of characters for user passwords.
- **Must contain uppercase and lowercase letters** – Requires passwords to contain an upper and lowercase letter.
- **Must contain both letters and numbers** – Requires passwords to contain both letters and numbers.
- **Days before passwords expire** – The number of days before a password must be changed, up to 365 days. Setting as zero means passwords will not expire.

Miscellaneous settings

On the **Standard** tab, select miscellaneous settings.

- **Server Identifier** – Sets the Evidence Local server name for files sent to another Evidence Local server with the Destinations feature. This is used to show the name of the server the file came from.
- **Hide inaccessible files in search results** – Hides search result files that users do not have rights to access. By default, this option is not selected, and inaccessible file results are highlighted in red.
- **Retention of inaccessible removed files (in days)** – How many days removed files are retained by the system.
- **Session Timeout** – The number of minutes an Evidence Local session can be inactive before the user is signed out. The default setting is 30 minutes, with a range of 15–480.

Interface configuration setting

On the **Standard** tab, select interface configuration settings.

- **Display Units** – Selects Imperial or Metric units.

Destination transfer settings

On the **Standard** tab, select destination transfer settings.

- **Concurrent Inbound Limit** – The maximum number of simultaneous transfers Evidence Local can receive from another Evidence Local instance. If the number of inbound transfers exceeds this limit, additional transfers are placed in a queued state until the active number of transfers is reduced.
- **Concurrent Outbound Limit** – The maximum number of simultaneous transfers Evidence Local can send to another Destination location. If the number of outbound transfers exceeds the concurrent limit, additional transfers are placed in a queued state until the active number of transfers is reduced.

Feature settings

On the **Standard** tab, select feature settings.

- **Use new image viewer** – Sets if the advanced image viewer is the default image viewer for Evidence Local. The advanced image viewer has options to rotate and zoom on the image.

After changing standard settings, remember to **Save**.

Schedule system settings

These settings let you schedule when Evidence Local will move and copy files. It is intended to prevent Evidence Local from consuming network bandwidth during high activity periods.

Reach these settings by selecting **Administration** from the [Quick menu](#) (page 3), then the **System Settings** tab.

1. Select the **Schedule** tab to create a storage schedule.
2. Edit an existing schedule by changing the settings in the appropriate schedule row or create a new schedule by selecting a blank row.
3. Select the **Day**, **Starting Time**, and **Duration** for the schedule:
 - **Day** – Set for a specific day (Monday, Tuesday, etc.), every day on Monday through Friday, or for every day. The default setting is Every Day.
 - **Starting Time** – Set for any time during the day, at 15-minute intervals on a 24-hour clock. The default setting is Midnight.
 - **Duration** – Set for any duration in intervals of 30 minutes. The default setting is 24 hours.
 - **Remove** – **Remove** the selected storage schedule.

After changing schedules, remember to **Save**.

Legacy system settings

Reach these settings by selecting **Administration** from the [Quick menu](#) (page 3), then the **System Settings** tab.

1. Select the **Legacy** tab.
2. Set the Home folders:
 - **Enable home folders** – Evidence Local will automatically create a Home folder for every user and an association for the user with the constraint of **User** and a folder of **Username**. Consider enabling this if you have a large number of users in your system. Default: disabled.
 - **Default storage location** – The default storage location for Home folders. The default location is named Default Storage Location.
 - **Default retention period (in days)** – The default retention time for Home folders. Default: 30 days.
 - **Post-retention workflow** – Sets the default post-retention workflow for Home folders. Default: Recycle Bin.

After changing legacy settings, remember to **Save**.