# Table of Contents

What's New ................................................................................................................................................ 14
Introduction ............................................................................................................................................... 15
   About This Guide ................................................................................................................................. 15
Administrator Overview ........................................................................................................................... 16
   Implementation Checklist ....................................................................................................................... 16
Supported Web Browsers .......................................................................................................................... 17
Sign In to Evidence.com ............................................................................................................................ 18
Dashboard ................................................................................................................................................. 18
   System Alerts ........................................................................................................................................ 19
   Critical Device Alerts ............................................................................................................................ 19
   Groups I Monitor ................................................................................................................................... 20
   Upcoming Evidence Deletions ................................................................................................................ 20
   System Usage ....................................................................................................................................... 21
   My Latest Uploads ............................................................................................................................... 22
   Evidence Shared with Me ....................................................................................................................... 23
   My Case Activity ................................................................................................................................... 23
Managing Your User Account ..................................................................................................................... 24
   Update Your Basic Account Information .............................................................................................. 24
   Verify Your Mobile Phone Number ....................................................................................................... 25
   Change Your Password .......................................................................................................................... 26
   Change Language ................................................................................................................................. 26
   Update Security Questions .................................................................................................................... 27
   Update Your Email Notifications ......................................................................................................... 28
Axon Citizen ............................................................................................................................................... 29
   Axon Citizen for Communities Workflow: ............................................................................................. 29
   Axon Citizen for Officers Workflow: ...................................................................................................... 30
   Axon Citizen Permissions and Settings Information ............................................................................. 30
      Example Axon Citizen Management Permissions ............................................................................ 32
   Citizen Evidence and Portal Details Page Overview .......................................................................... 32
   Creating a Public Portal .......................................................................................................................... 36
   Editing a Public Portal ............................................................................................................................ 38
Closing a Public Portal..............................................................................................................................................39
Instructions for Evidence Collectors..........................................................................................................................39
   Using Axon Capture to Invite an Individual ...........................................................................................................39
   Using Evidence.com to Invite an Individual ..........................................................................................................41
Virus Scan for Axon Citizen ........................................................................................................................................43
Submission Notifications .............................................................................................................................................43
Using Evidence.com to Triage Submissions ................................................................................................................44
Searching for Axon Citizen Evidence in Evidence.com ............................................................................................46
   Additional Information on Citizen Evidence Detail Pages ..................................................................................46
What Community Members See ..................................................................................................................................48
   Public Portal .........................................................................................................................................................48
   Individual Invite – Phone ......................................................................................................................................49
   Individual Invite - Email ......................................................................................................................................51
Evidence Management..................................................................................................................................................54
   Import Evidence ..................................................................................................................................................54
   Evidence Search — All Evidence, My Evidence, and Shared Evidence ...............................................................55
      Evidence Search Filters ......................................................................................................................................57
Working with Evidence Search Results ........................................................................................................................60
   View Evidence .......................................................................................................................................................60
   Request Access ....................................................................................................................................................61
Adding Users and Groups to the Inside My Agency Access List from the Evidence Search Page ................................62
Adding Users and Groups to an Outside My Agency Access List from the Evidence Search Page ................................64
Providing Evidence Outside My Agency by Unauthenticated Download Link from the Evidence Search Page ..........66
Restricting Evidence from the Evidence Search Page ................................................................................................68
Update ID .................................................................................................................................................................70
Add Category to Evidence ..........................................................................................................................................70
Reassign Evidence .......................................................................................................................................................71
Bulk Video Redaction .................................................................................................................................................71
Bulk Download Evidence .........................................................................................................................................73
Download Speed Information .......................................................................................................................................75
Delete Evidence................................................................................................................................ 75
Restore Evidence.............................................................................................................................. 76
Export Evidence Search Results..................................................................................................... 77
Working with Any Evidence..................................................................................................................... 77
Adding Users and Groups to the Inside My Agency Access List from the Evidence Detail Page .......................................................... 78
Modifying Inside My Agency Access Information .............................................................................. 80
Removing Users and Groups from the Inside My Agency Access List .............................................. 82
Adding Users and Groups to the Outside My Agency Access List .................................................... 83
Modifying and Removing Users and Groups from Outside My Agency Access Lists .................. 86
Restricting Evidence from the Evidence Detail Page ........................................................................... 88
Removing Restriction from Evidence ............................................................................................... 92
Edit Title and ID ............................................................................................................................. 92
Edit Recorded Date and Time .......................................................................................................... 93
Download Evidence File .................................................................................................................. 93
Flag or Un-Flag Evidence ................................................................................................................ 94
Add to or Remove Evidence from a Case ...................................................................................... 94
Reassign Evidence ........................................................................................................................ 95
View Evidence Audit Trail .............................................................................................................. 95
Delete Evidence ............................................................................................................................. 96
Restore Deleted Evidence ............................................................................................................... 96
Assign and Un-Assign Categories .................................................................................................... 97
Add and Remove Tags for Evidence .............................................................................................. 97
Edit Location ..................................................................................................................................... 98
Edit Description ................................................................................................................................ 99
Notes and Evidence ......................................................................................................................... 99
View Evidence with Same ID ........................................................................................................... 100
Viewing Video Source Information .................................................................................................. 100
Viewing Document Evidence ........................................................................................................... 101
PDF Viewer Controls ...................................................................................................................... 101
PDF Viewer Actions ......................................................................................................................... 101
Playing Video and Audio Evidence ............................................................................................... 102
Supported File Types ...................................................................................................................... 102
Run a Report .......................................................................................................................................... 207
Downloading Reports ........................................................................................................................... 209
  Download Report from Reports Page ........................................................................................ 209
  Download Report from Email Download Link ........................................................................... 209
Example Data Aggregation Using Microsoft Excel Pivot Tables ...................................................... 209
Administrator Overview ......................................................................................................................... 211
User Administration ............................................................................................................................... 211
  User Account Statuses .......................................................................................................................... 212
    User Account Added as Active ........................................................................................................ 213
    User Account Added as Inactive ....................................................................................................... 213
    Active User Account During Password Reset ............................................................................ 213
  Add Users ............................................................................................................................................... 213
    Add One User ................................................................................................................................ 214
    Add Many Users ............................................................................................................................ 215
  Complete the User Registration Process ........................................................................................... 217
  Re-Invite Users ..................................................................................................................................... 218
  Deactivate Users ............................................................................................................................... 218
    Deactivate Many Users .................................................................................................................. 219
    Deactivate One User ..................................................................................................................... 220
  Reactivate Users .................................................................................................................................... 221
  Unlock a User Account ........................................................................................................................ 221
  Reset Passwords and Security Questions .......................................................................................... 222
    Reset Password and Security Questions from a User Details Page ....................................... 222
    Reset Passwords and Security Questions for Users from User Search Results ................... 223
  Send a Message to a User .................................................................................................................... 223
  Change a Username ............................................................................................................................. 224
  Edit Other User Account Information ............................................................................................. 224
  User Audit Trail ...................................................................................................................................... 225
    Get a User Audit Trail ....................................................................................................................... 227
  Expire All Passwords ........................................................................................................................... 227
Groups Administration ............................................................................................................................ 228
  Groups and Membership ...................................................................................................................... 228
  Managing Group Access ....................................................................................................................... 229
What’s New

This guide includes the following changes, made in support of the October 2018 updates to Evidence.com:

- Updated Axon Citizen – Citizen Evidence and Portal Details Page Overview section with information about Owner column and filters.

- Updated the Evidence Search Filters – Advanced Search Filters section with information on the new Source filter.

- Added a procedure to Add Multiple New Vehicles for Axon Fleet 2 and Axon Fleet to the Vehicle search section.

- Updated the Early Access Devices section to include Axon Flex 2 cameras and controllers as early access devices.

- Updated descriptions of special categories with the following changes – the Uncategorized category can have an evidence retention policy setting and Pending Review can be a restricted category.

For more information about the most recent release, see the following document:

- Evidence.com October 2018 Release Notes

For further information about changes to this guide, see Revision History.
Introduction

Axon Enterprise, Inc. (Axon) has developed the Axon system and Evidence.com solution for use by law enforcement. Depending on agency need, the solution can provide on-officer video capture, secure digital media storage and management, and paperless tracking and reporting. This unique system is suitable for both smaller agencies lacking in resources or large agencies trying to streamline and become more economical.

Note: For more information on the Axon system, see www.axon.com.

The solution consists of three core parts: capture, transport, and data management.

Capture

The capture element is an on-officer camera designed to capture video from the officer’s perspective. Axon Flex and Axon Body 2 integrate easily with Evidence.com.

Transport

The transport element consists of Axon Dock and the Evidence Sync PC desktop application. Axon Dock functions as the docking, charging, and upload station for the Controller and the DVR. The Evidence Sync application provides a secure interface for uploading and managing TASER Conducted Electrical Weapon (CEW) generated logs as well as TASER CAM and Axon videos.

Note: TASER has changed the generic term describing our handheld products from Electronic Control Device (ECD) to Conducted Electrical Weapon (CEW).

Data Management

Evidence.com services provide a secure and easily accessed interface for management, sharing and viewing of mission critical data. Unlike other data management solutions, the Evidence.com website provides the first Software as a Service (SaaS) solution for law-enforcement data management. Using cloud architecture and infrastructure, Evidence.com services require minimal infrastructure improvements by the agency.

About This Guide

This guide is a reference for Evidence.com users and administrators.

For users, the guide includes information on using Evidence.com to work with data and manage your Evidence.com account. The actions you can take in Evidence.com depend on the permissions granted to you by your agency’s Evidence.com administrator.
For Evidence.com agency administrators, the guide includes information to assist with setting-up and administer on-going operations of your agency.

If you require additional assistance, contact Technical Support via support@axon.com or at 800-978-2737 ext 2 or +1 480-463-2170.

**Administrator Overview**

An administrator account is created for every agency on Evidence.com during the initial implementation cycle. The username of this administrator account is the email address that your organization specified.

Typically, the person most responsible for your Evidence.com agency owns the first administrator account. The first administrator usually defines security settings, creates custom roles and permissions, adds users (User, Administrator, Armorer or any other custom roles), reassigns devices, creates categories and sets retention policies, and configures several other administrative features of your Evidence.com agency.

**Implementation Checklist**

The following list is a brief summary of implementation tasks for administrators of a new Evidence.com agency:

**Note:** The availability of features depends on your Evidence.com agency type.

- Confirm administrator status in Evidence.com
- Confirm agency profile information
- Configure custom [Roles and Permissions](#) (optional)
- Configure account settings
  - Configure and [add users](#)
  - Confirm and [adjust device (camera, CEW, etc.) settings](#) as needed
  - Configure [Categories and Retention Policies](#)
  - Configure [Evidence ID validation](#) (optional)
  - Enable [IP address security](#) (optional)
- Enable multi-factor authentication (optional)
- Configure password settings (optional)

## Supported Web Browsers

Evidence.com supports the use of the following web browsers:

- Internet Explorer version 11

**Note:** If you use Internet Explorer 11, ensure that Compatibility View is disabled. Evidence.com does not support the use of the Compatibility View feature. To verify your Internet Explorer settings, go to Tools > Compatibility View settings and ensure that Evidence.com is not included in the list of websites added to Compatibility View and that the “Display all websites in Compatibility View” check box is cleared. Additionally, ensure that Font download is enabled. Evidence.com uses custom fonts and disabling Font download will prevent the display of information. To verify your Internet Explorer settings, go to Tools > Internet Options, select the Security tab and click the Internet zone. In the Security level for this zone section, click Custom level and, under the Downloads settings, verify that Font download is set to Enable.

- Microsoft Edge
- Chrome version 40 and above
- Firefox version 30 and above
- Safari version 8 and above

Additionally, Evidence.com supports the media player and related tools, introduced in Evidence.com release 1.27, with the following web browsers:

- Internet Explorer version 11
- Chrome version 43 and above
- Firefox version 38 and above
- Safari version 8 and above

If you use an unsupported browser to access media-evidence files, Evidence.com provides the traditional media player.

It is strongly recommended that you always use the latest release of Adobe Flash.
Sign In to Evidence.com

To sign in to Evidence.com, you must go to your agency’s Evidence.com page.

1. In a web browser, go to your agency’s unique URL:

   https://youragencyname.evidence.com

   Your agency's sign in page appears.

   If you do not know your agency URL, enter evidence.com in your browser address bar and then enter your email address and click Search to find your agency. If you are still unable to find your agency, contact Customer Service at 1-800-978-2737 or your Axon sales engineer for assistance.

2. In the Username and Password boxes, type the required information.

   You can enter your assigned username or email address in the Username field.

3. Click Sign In.

4. If Evidence.com challenges you for a security code or answers to your security questions, type the required information and then click Sign In again.

   Note: If you sign in to Evidence.com while you are already signed in from another location, Evidence.com terminates the original session.

Dashboard

The Dashboard appears when you sign in to your Evidence.com agency. You can also return to the Dashboard page from any other area in Evidence.com by clicking the Axon logo (▲) in the upper-left corner of the page.

The Dashboard includes the following sections:

Note: Depending on your role and permissions, you may not see all of these sections.

- System Alerts
- Critical Device Alerts
- Citizen Evidence (see Axon Citizen for more information)
- Groups I Monitor
- Upcoming Evidence Deletions — User Initiated and System Initiated
- System Usage
- My Latest Uploads
- Evidence Shared with Me
- My Case Activity

**System Alerts**

The System Alerts section informs administrators about the status of their agency’s Evidence.com Security Settings. These warnings alert administrators if a recommended security feature is not enabled.

If all recommended security features are enabled, the System Alerts section is empty.

If you want to clear an alert, to the right of the alert, click **Update**. The applicable page opens and you can configure the security feature. For example, for the IP Restriction warning, clicking Update opens the security settings page for IP security.

For information about configuring each security feature, see the applicable section in this guide, such as [IP Security](#).

![SYSTEM ALERTS](warning-icon)

**Critical Device Alerts**

The Critical Device Alerts section lists up to five devices that are reporting problems.

It is recommended that you do not use devices listed under Critical Device Alerts and that you contact customer service immediately.

If none of your agency’s devices have a critical error status, “No Results Found” appears in this section.
If you want to see all devices that have an error status of Critical, in the upper-right corner of the Critical Device Alerts section, click **View all**.

![Critical Device Alerts Table]

**Groups I Monitor**

The Groups I Monitor section lists groups for which you have evidence-monitoring permission. To access the profile page for a group, click the group title.

![Groups Monitor Table]

**Upcoming Evidence Deletions**

The Upcoming Evidence Deletions section includes two lists:

- **User Initiated** — Lists evidence that has been manually scheduled for deletion.

- **System Initiated** — Lists evidence automatically scheduled for deletion in accordance with the retention duration of the category that is assigned the evidence. For more information, see [Categories and Evidence Retention Policies](#).
Each list shows five evidence files at a time. To move through a list, use the pagination controls below the list.

### User Initiated

<table>
<thead>
<tr>
<th>TITLE</th>
<th>OWNER</th>
<th>DELETION DATE</th>
<th>OPTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audio 16:06-12:31:1103050</td>
<td>Chiles, Bryan</td>
<td>Queued for deletion</td>
<td>Restore</td>
</tr>
<tr>
<td>Photo 16:09-12:31:145959</td>
<td>ADMIN, Phil</td>
<td>Queued for deletion</td>
<td>Restore</td>
</tr>
<tr>
<td>Photo 16:09-12:31:155959</td>
<td>ADMIN, Phil</td>
<td>Queued for deletion</td>
<td>Restore</td>
</tr>
<tr>
<td>Photo 16:09-12:31:159959</td>
<td>ADMIN, Phil</td>
<td>Queued for deletion</td>
<td>Restore</td>
</tr>
<tr>
<td>Photo 16:09-12:31:159959</td>
<td>ADMIN, Phil</td>
<td>Queued for deletion</td>
<td>Restore</td>
</tr>
</tbody>
</table>

If you want to view the details of an evidence file, click the evidence title.

If you want to prevent evidence from being deleted, the process is different for user-initiated evidence and system-initiated evidence.

- To restore evidence from the User Initiated list, click Restore and then, on the confirmation message box, click OK.

- To restore evidence from the System Initiated list, click the evidence title and then assign the evidence a category with a retention duration that prevents the deletion of the evidence. For more information, see Categories and Evidence Retention Policies.

### System Usage

The System Usage summary and graph summary includes the amount of usage broken out by video, audio and other types expressed in gigabytes (GB).

It displays the amount of evidence added and deleted by your agency's users as well the average (net) in the last 30 days.
It also displays the total number of Evidence.com users and your agency’s active devices.

My Latest Uploads

My Latest Uploads lists the most recent evidence and log files uploaded to your account from Axon and TASER devices, or other external devices.

If you want to see all your evidence, in the upper-right corner of the My Latest Uploads section, click View all.

If you want to view the details of an evidence file, click the evidence title.

If you want to see a list of all evidence with the same ID as an evidence file in the list, click the evidence ID.

Under Actions, you can view the evidence audit trail, download the evidence, flag the evidence, or delete the evidence.
Evidence Shared with Me

The Evidence Shared with Me page lists up to 10 evidence files that have been shared with you. The list shows the ID, title, file type, owner, sharing duration, and sharing expiration date.

If you want to see all evidence shared with you, in the upper-right corner of the Evidence Shared with Me section, click View all.

If you want to view the details of an evidence file, click the evidence title.

If you want to see a list of all evidence with the same ID as an evidence file in the list, click the evidence ID.

<table>
<thead>
<tr>
<th>ID</th>
<th>Title</th>
<th>File Type</th>
<th>Owner</th>
<th>Duration</th>
<th>Expiration Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>2112</td>
<td>Old Guys Playing</td>
<td>Image</td>
<td>Buti, Kuba</td>
<td>N/A</td>
<td>13 Aug 2015 - 08:30:39</td>
</tr>
<tr>
<td>131313</td>
<td>Bird Feeder</td>
<td>Image</td>
<td>Buti, Kuba</td>
<td>N/A</td>
<td>13 Aug 2015 - 11:10:17</td>
</tr>
<tr>
<td>2112</td>
<td>On Screen</td>
<td>Image</td>
<td>Drummond, DB</td>
<td>N/A</td>
<td>24 Aug 2015 - 15:48:16</td>
</tr>
<tr>
<td>2112</td>
<td>Summary</td>
<td>Image</td>
<td>Drummond, DB</td>
<td>N/A</td>
<td>24 Aug 2015 - 15:48:16</td>
</tr>
<tr>
<td>Cats</td>
<td>Moat</td>
<td>Image</td>
<td>Hamish, HC</td>
<td>N/A</td>
<td>05 Oct 2015 - 15:42:21</td>
</tr>
<tr>
<td>StalingFrist</td>
<td>1B</td>
<td>Image</td>
<td>Hamish, HC</td>
<td>N/A</td>
<td>23 Oct 2015 - 10:45:24</td>
</tr>
<tr>
<td>2112</td>
<td>Backyard</td>
<td>Image</td>
<td>Hamish, HC</td>
<td>N/A</td>
<td>23 Oct 2015 - 10:45:23</td>
</tr>
</tbody>
</table>

My Case Activity

My Case Activity displays up to 10 cases that you have created along with their status, creation date, and the date they were last updated.

If you want to see all your cases, in the upper-right corner of the My Case Activity section, click View all.

If you want to view the details of a case, click the case ID.
Under Actions, you can flag cases or delete them.

## Managing Your User Account

Users can update many settings for their own user accounts.

If you do not want to allow users to perform any of the procedures in this section, such as changing username and email address, ensure that the role that you assign to users prohibits the Edit Account Information permission.

**Note:** The default permissions assigned to the User role does allow the Edit Account Information permission. For more information about permissions in pre-configured user roles, see Appendix A: Roles and Permissions.

## Update Your Basic Account Information

Basic account information that you can update includes items such as the following:

- Username
- First Name
- Last Name
- Badge ID
- Cell Phone Number
- Email address
• **Time Zone**

1. In the upper-right corner of the page, click your user name.

   ![User Account Display](image)

   Evidence.com displays the Accounts and Passwords page for your user account.

2. Under **User Information**, make the changes that you need.

   **Note:** You cannot verify an updated phone number until you have saved the changes.

3. Click **Save**.

   Above User Information, a banner message about the success of the updates appears.

---

### Verify Your Mobile Phone Number

For multi-factor authentication, you can enable Evidence.com to send one-use security codes to your mobile phone.

After you add a mobile phone number or change the mobile phone number on your user account, Evidence.com considers the number unverified. Before Evidence.com can send security codes to your phone, you must verify the phone number.

1. Click your name, in the upper-right corner, to go to the User Information page.

   ![User Account Display](image)

   Evidence.com displays the Accounts and Passwords page for your user account.

2. Enter in your mobile phone number in the **Cell Phone** field and save the change.

   **Note:** If Verified is shown adjacent to your mobile phone number, no further action is needed.

3. Click **Send Verification Code**.

   A dialog box displays the verification method options, which are a voice call or a SMS (text) message.

4. Select the method for how you want to receive your security code.
A dialog box for submitting the verification code appears and Evidence.com sends the verification code to the phone number saved in your user account.

5. Use your mobile phone to receive the verification code.

6. In the **Code** box, type the verification code and then click **OK**.

7. On the notification message box, click **OK**.

Your mobile phone is verified and this completes your preparation to use multi-factor authentication.

---

**Change Your Password**

You can change your password as needed.

1. In the upper-right corner of the page, click your user name.

Evidence.com displays the Accounts and Passwords page for your user account.

Under Change Password, the boxes for changing your password appear.

2. In the **Current Password**, **New Password**, and **Confirm New Password** boxes, type the required information.

3. Click **Save Password**.

Above Change Password, a banner message notifies you about the success of the password change.

---

**Change Language**

You can choose the language that you see for all labels in your Evidence.com agency. Your agency has a default language that is set for every user when your Evidence.com agency was created. The language setting offers you the option to change the default language to the language that you are most comfortable using.

**Note:** If the language option is not available on the Accounts and Passwords page for your user account, then your organization has requested that the feature be disabled for your Evidence.com agency.
1. In the upper right corner of the page, click your user name.

The Account and Password page appears.

1. Under **User Information**, in the **Language** list, click the language that you want to use and then click **Save**.

2. Sign out and then sign in to your Evidence.com agency again.

   The Evidence.com pages use the language that you selected.

---

**Update Security Questions**

You can update your security questions as needed.

1. In the upper-right corner of the page, click your user name.

The Accounts and Passwords page appears.

2. On the second menu bar, click **Security Questions**.

   The Security Questions page appears. For security purposes, the page does not show your current security question configuration.

3. For each security question list, click the question that you want to use and then type the answer in the box below the list.

   The two questions cannot be the same; otherwise, Evidence.com does not allow you to save your changes.

4. In the **Current Password** box, type your password.

5. Click **Save** and then, on the notification message box, click **OK**.
Update Your Email Notifications

You can set personal preferences for email notifications. The email notifications that are available to you are determined by the role assigned to your user account. You may not see all of the email notification settings.

Evidence.com supports the following email notification settings:

- **Account Lockout Notification** — Turn on to receive an email if Evidence.com locks your account because you exceeded the maximum number of incorrect login attempts.

- **External Agency Collaboration Notifications** — Turn on to receive notifications regarding other agencies that would like to collaborate with you and share evidence.

- **Evidence Delete Digests Notification** — Turn on to receive an email with the summary of upcoming evidence deletions for the next week in your Evidence.com Inbox.

- **Incorrect Capture Date Notification** — Turn on to receive an email informing you about any evidence uploaded by your agency that appears to be recorded more than 14 days ago, which could be indicative of a device with a system clock in need of synchronization with Evidence.com.

- **Category Assignment Notification** — Turn on to receive an email when evidence uploaded is also assigned to at least one category that is in the process of being deleted. This notification helps ensure that no evidence is unintentionally deleted during system-initiated evidence deletions.

- **Signal Sidearm Low Battery Notification** — Turn on to receive an email when your assigned Signal Sidearm device has a low battery.

1. In the upper-right corner of the page, click your user name.

   ![User Profile](image)

   The Accounts and Passwords page appears.

2. On the second menu bar, click **Notifications**.

   If your role allows you to receive email notifications, a setting for each allowed notification appears.

   If your role does not allow any email notifications, the page includes a “Your role currently doesn’t have any email notification enabled” message.
3. For each email notification that you want to change, click on the associated switch to turn on or off the notification as needed.

Axon Citizen

Axon Citizen makes it easy for law enforcement agencies to securely receive evidence submissions from the community and manage that media in Evidence.com. Axon Citizen has two components:

- Axon Citizen for Communities allows agencies to create public evidence submission portals where the public can submit evidence during both large-scale and smaller, day-to-day events.

- Axon Citizen for Officers allows officers to send out individual invites to witnesses directly from Axon Capture or Evidence.com.

Outlines of the Axon Citizen for Communities and Axon Citizen for Officers workflows are provided below:

Axon Citizen for Communities Workflow:

1. Create Public Portal when you need the community’s help.

2. Post the portal link to your website, social media, news outlets, etc.

3. Community members upload files and Evidence.com notifies the portal creator about new submissions.

4. Triage submissions to determine what to accept and decline.

5. Leverage existing tools to manage evidence submissions (search, sharing, access control, redaction, audit trails).
Axon Citizen for Officers Workflow:

1. Invite individual from Axon Capture or Evidence.com

2. The community member uploads files and Evidence.com notifies the officer about the submission.

3. If enabled at agency, triage submissions to determine what to accept and decline.

4. Leverage existing tools to manage evidence submissions (search, sharing, access control, redaction, audit trails).

Agencies can choose to allow community member submissions to be automatically added as evidence or to use the triage workflow to allow the evidence owner to accept or decline the submissions. The owner of the evidence is the officer that sent the invitation.

Agencies that let users decline evidence submissions can also choose to set a custom retention period for all declined evidence submissions. The custom retention period determines when the declined submissions are queued for deletion, similar to the category retention setting in Evidence.com. If a custom retention period is not set, the declined evidence will use existing agency retention categories to determine when the evidence will be queued for deletion.

Axon Citizen Permissions and Settings Information

Before users can create public portals, send individual invitations, and use the triage workflow, agency Evidence.com administrators must modify or create new Roles and enable the appropriate Axon Citizen permissions for the Roles.

Users that will use Axon Citizen with Axon Capture must have the Login Access permission for Axon Capture is set to **Allowed**.
The Citizen Management permissions are described below. See [Example Axon Citizen Management Permissions](#) for some example permission use cases.

<table>
<thead>
<tr>
<th>Citizen Management</th>
<th>Access</th>
<th>Portals Access</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Portals</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Individual &amp; Public)</td>
<td>ANY PORTAL</td>
<td>ONLY THEIR OWN</td>
<td>PROHIBITED</td>
</tr>
<tr>
<td>Invite Individual</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Create Public Portal</td>
<td>ANY PORTAL</td>
<td>ONLY THEIR OWN</td>
<td>PROHIBITED</td>
</tr>
<tr>
<td>Edit and Close Public Portal</td>
<td>ANY PORTAL</td>
<td>ONLY THEIR OWN</td>
<td>PROHIBITED</td>
</tr>
<tr>
<td>Triage Submissions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Trail PDF</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **View Portals (Individual & Public):** Allows a user to view information about a portal, but not edit the information or view triage submissions. This can be set to allow the user to view any portal or only portals created by the user.

- **Invite Individual:** Allows a user to create an individual portal for an individual citizen.

  To enable this permission, the View Individual & Public Portal permission cannot be set to Prohibited.

- **Create Public Portal:** Allows a user to create a public portal that can be used by the community to upload items.

- **Edit and Close Public Portal:** Allows a user to edit and close (make inactive) a public portal. This can be set to allow the user to edit or close any portal or only the portals created by the user.

  To enable this permission, the View Portals permission must be set to Any Portal or Only Their Own. If the Role has Only Their Own View Portals permission, then the user can only select Only Their Own for the Edit and Close Public Portal permission.

- **Triage Submissions:** Allows a user to accept or decline items from individual invites and public portal submissions. This can be set to allow the user to triage submissions from any portal or only from portals created by the user.

  To enable this permission, the View Portals permission must be set to Any Portal or Only Their Own. If the Role has Only Their Own View Evidence permission or Only Their Own View Portals permission, then the user profile is limited to Only Their Own for the Triage Submissions permission.

- **Audit Trail PDF:** Allows user to view and download a PDF record of who has viewed, edited or triaged portals.

  To enable this permission, the View Portals permission must be set to Any Portal or Only Their Own.
Agency Evidence.com administrators should set up the agency Axon Citizen settings as needed for your Axon Citizen implementation before allowing users to create public portals or send individual invitations. See Citizen Settings for more information on the settings.

Example Axon Citizen Management Permissions

The following table provides some example Role permission settings for using Axon Citizen based on different use cases. The Audit Trail PDF permission setting should be determined by your agency policies for reviewing audit trails.

<table>
<thead>
<tr>
<th>Use case</th>
<th>View portal</th>
<th>Invite individual</th>
<th>Create public portal</th>
<th>Edit and close public portal</th>
<th>Triage submissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patrol officers that can invite individuals and must triage their own submissions</td>
<td>Only Their Own</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Only Their Own</td>
</tr>
<tr>
<td>Detectives that can create public portals and triage their own submissions.</td>
<td>Only Their Own</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Only Their Own</td>
<td>Only Their Own</td>
</tr>
<tr>
<td>Someone in the public information office that can create a public portal, but not triage themselves.</td>
<td>Any Portal</td>
<td>Prohibited</td>
<td>Allowed</td>
<td>Any Portal</td>
<td>Prohibited</td>
</tr>
<tr>
<td>You have a centralized group that can triage any portal.</td>
<td>Any Portal</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Any Portal</td>
</tr>
<tr>
<td>Command staff that can access and triage any portal.</td>
<td>Any Portal</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Any Portal</td>
<td>Any Portal</td>
</tr>
</tbody>
</table>

Citizen Evidence and Portal Details Page Overview

To assist with managing submissions from individual invitations, the Citizen Evidence page has been added to the Evidence tab. The Citizen Evidence page lists information about to public portals and individual invites the user can access and provides links to Portal Details pages. Each list shows a maximum of 10 entries, with page numbers and navigation arrows below each list. Users can click a page number or use the navigation arrows to change the list results.
Users assigned to roles that have the View Portals (Individual & Public) permission set to Any Portal, will also see a Show/Hide Filters option. When Show Filter is clicked, a toggle switch is shown that allows the user to only show portals they own or show all the portals at the agency.

This page also provides links to create new public portals and individual invites.

The Portal Details pages provide general information about a public portal or individual invites. The information for portals and individual invites that have items to triage are in bold text and there is a blue indicator bar on the left-side of the entry. Users can access a Portal Details page by:
• Clicking **View Submission** in the email message they receive from Evidence.com after a submission is uploaded.

• In Evidence.com on the menu bar, click **Evidence**, then click **Citizen Evidence**. In the Public Portals or Individual Invites list, find the page you want to view and then click **View Summary** in the Portal Info column.

Portal Details pages for individual invites and public portals display similar information, but with some differences due to the additional requirements for public portals.

The Portal Details Page for an individual invite shows the following information:

- A summary of evidence submissions and whether any items require triage. Each summary item with a value is a link. Clicking the link takes you to an Evidence Search page with evidence associated with the portal. The evidence shown is filtered based on the link clicked.
  
  If there are untriaged items in the submission, a button to review submissions is shown.

- A link to the portal Audit Trail.

- Invite information (created on, created by, associate categories, etc.).

- An Evidence List showing the submitted items.
The Portal Details page for a public portal shows the following information:

- A summary of evidence submissions and whether any items require triage. Each summary item with a value is a link. Clicking the link takes you to an Evidence Search page with evidence associated with the portal. The evidence shown is filtered based on the link clicked.

  If there are untriaged items in the submission, a button to review submissions is shown.

- Portal settings information (title, ID, categories, etc.).

- A link to the portal Audit Trail.

- An option to visit the portal, which opens the portal view shown to community members in a new browser tab.

- A toggle switch to close and reopen the portal.

- Public link information for sharing the public portal with new organizations, social media and other websites.

- The location information and map, if the location was added to the portal.

- The ID information for the current portal owner, the date the portal was created, and the ID information for the user that created the portal.
Creating a Public Portal

1. Sign in to your Evidence.com account.

2. On the dashboard page, under Citizen Evidence, click **Create Public Portal**.

   Alternately, on the menu bar, click **Evidence**, then click **Citizen Evidence**, and then click **Create Public Portal**.

   The Create Public Portal page opens.

3. In the **Public URL** field, enter the incident url. The incident url must be unique and you cannot use upper case letters, spaces, or special characters in the incident url.

   This text is appended to your agency's public url to create the specific url path for the incident. Axon recommends using text that is similar or related to the portal Title.

4. Enter the **ID** as required by your agency.

5. Add evidence **Categories** as needed. A public portal can have multiple categories.
6. Enter the **Portal Owner** information. The Portal Owner is the user that can view and edit portal settings, triage portal submissions, receive email notifications when a submission is added to the portal, and the user will be assigned incoming portal evidence.

When a user is assigned as a portal owner, Evidence.com sends the user an email notification informing them that they are the portal owner. The portal owner can be different than the user creating the portal.

7. Enter a **Title** for the portal. The title is used in the Evidence.com Public Portal list and as part of the title community members see on the portal welcome page. The title can have a maximum of 127 characters.

8. Enter a **Description** for the portal. The description text is used on the portal welcome page and social media sites. The description can have a maximum of 2,000 characters. The text automatically wraps on the screen, but you can manually insert line breaks using your keyboard Enter key.

9. Optionally, add a **Date and Time**. This information can make it easier for triagers to compare the submissions to the incident.

10. Optionally, click the edit icon (image placeholder) in **Location of Incident** to add a location. The location box expands to show a map.

- Enter the **Address** of the incident or click on the map to set the address.
- Optionally, enter a friendly name for the location.
- Click **Save**.
11. Click **Submit**.

You are taken to the Portal Details Page. From here you can copy and share the portal link on social media and other websites. The Portal Details Page is also used to close the portal when it is no longer needed.

**Editing a Public Portal**

1. Sign in to your Evidence.com account.

2. On the menu bar, click **Evidence**, then click **Citizen Evidence**, and then click the **View Summary** link for the portal you want to change.

   The Portal Details page opens.

3. Click the edit (📝) icon.

   The Edit Public Portal page with the current portal information is shown.

4. Change the portal information as needed.

   Changes to any fields must meet the same requirements as when [creating a portal](#).

5. Click **Save**.
You are taken to the Portal Details Page. From here you can copy and share the portal link on social media and other websites. The Portal Details Page is also used to close the portal when it is no longer needed.

### Closing a Public Portal

1. Sign in to your Evidence.com account.
2. On the menu bar, click **Evidence**, then click **Citizen Evidence**, and then click the **View Summary** link for the portal you want to close.

   The Portal Details page opens.

3. Under the Share Public Link heading, toggle the switch to say **Closed for Submissions**.

4. This closes the portal and the link is no longer active.

   If someone clicks the link, they will get a Page Not Found message in their browser.

   The portal can be re-opened later by toggling the switch.

### Instructions for Evidence Collectors

There are two ways to invite an individual, using Axon Capture and using Evidence.com. Evidence.com is used to manually triage and accept or decline evidence submissions, if required by your agency.

To prevent spam, each private link can only be used for one submission. Each submission is limited to a maximum of 16 files, with a maximum size of 60 GB per file and a total submission size of 200 GB. The private link for submissions expires after 3 days.

**Note:** For agencies that have French set as their default language in Evidence.com, the Axon Citizen individual invite text, Terms of Use, and Privacy Policy information will also appear in French.

### Using Axon Capture to Invite an Individual

This section provides an overview of sending an Axon Citizen invitation through Axon Capture.
Note: The user must be allowed to invite individuals with Axon Citizen in Evidence.com and have Axon Capture for Android version 3.6 or later or Axon Capture for iOS version 3.7 or later to invite an individual.

1. Open the Axon Capture app.

2. Go to the Capture screen and tap Citizen.

3. On the Invite Individual screen, enter the Incident ID or NA, as required by your agency.

4. Add Categories as needed. An individual invite can have multiple categories.

5. Select if the invitation will be sent to a Phone (text message) or Email.
   - For phone numbers, select the country code and enter the Phone for the community member submitting items.
   - For email, enter the Email for the community member submitting items.

6. If allowed by your agency, you can select to store a contact’s information in Evidence.com.
If email was selected as the delivery method, the contact's information is always stored in Evidence.com.

If your agency requires contact information to be stored in Evidence.com, this option will not be shown.

7. If the contact's information should be stored, enter the name and birth date information for the contact.

8. Tap Send.

The invite is sent to the phone number or email address. The message contains a one-time use link to a website where the citizen can upload video, photo, and audio files for submission.

After the contact uploads the submission, you will receive an email message from Evidence.com. If your agency requires you to triage submissions, you can use the link in the email to go to the triage page for the submission.

9. On the Invite Sent screen, you can:
   - Tap OK to return to the main Capture screen.
   - Tap Create another invite to use the same Incident ID and Categories for a new invitation. Repeat steps 5 through 7 and tap Send to send a new invite.

**Using Evidence.com to Invite an Individual**

1. Sign in to your Evidence.com account.

2. On the dashboard page, under Citizen Evidence, click Invite Individual.

   Alternately, on the menu bar, click Evidence, then click Citizen Evidence, and then click Invite Individual.
3. On the Individual Invite page, enter the ID or NA as required by your agency.

4. Add Categories as needed. An individual invite can have multiple categories.

5. Select the Delivery Method, either Text message or Email.
   - For Text message, select the country code and enter the Mobile Phone Number for the community member submitting items.
   - For email, enter the Email address for the community member submitting items.

6. If allowed by your agency, select if the contact's information should be stored in Evidence.com.
   - If email was selected as the delivery method, the contact's information is always stored in Evidence.com.
   - If the information should be stored, enter the name and birth date information for the contact.

7. Click Submit.
   - The invite is sent to the phone number or email address. The message contains a one-time use link to a website where the citizen can upload video, photo, and audio files for submission.
   - After the contact uploads the submission, you will receive an email message from Evidence.com. If your agency requires you to triage submissions, you can use the link in the email to go to the triage page for the submission.
8. Click **Done** in the Successfully Created Portal dialog box to return to the Individual Invite page.

**Virus Scan for Axon Citizen**

Because it is critical to limit the possibility of viruses, files submitted through Axon Citizen links will undergo a scan for viruses when the files are ingested into Evidence.com. Files that pass the scan can be managed normally in Evidence.com, like any other evidence.

If a file has been submitted and the virus scan is still in progress, a warning is shown if a user tries to download the file.

When a file fails the virus scan, Axon notifies your agency's Evidence.com administrators that there is an issue with the file.

Files that failed the scan can only be downloaded by users with Download Infected Files permission set to Allowed. In this situation, the user is shown a warning message informing them that the file did not pass the virus scan. If they want to download the file, the user selects a check box acknowledging the risk and can download the file.

Files and Cases with files that did not pass the virus scan can be shared inside your agency, with partner agencies, and by download link. Additional controls around sharing files that failed a virus scan will be added in future releases.

**Submission Notifications**

Each time a submission is received for a public portal or individual invite, Evidence.com sends an email notification to the owner. However, for public portals, if Evidence.com
receives additional submissions for a portal before the user visits and triages the portal, then additional emails are not sent to that user.

Using Evidence.com to Triage Submissions

Note: The triage workflow is not supported for Internet Explorer 11 on Windows 7 platforms.

Use the following procedure to review and accept or decline community submissions.

1. Go to the Portal Details Page for the submissions you want to triage. You can get to the page by:
   - Click **View Submission** in the email message you receive from Evidence.com after a submission is uploaded. The email lists the ID, categories, and number of untriaged items in the submission.
   - In Evidence.com, on the menu bar, click **Evidence**, then click **Citizen Evidence**. In the My Individual Invites list, find the invitation you want to view and then click the Portal Info link.

You are taken to the Portal Details Page.

Note: The example image below shows a Public Portal Detail Page. Individual invite pages show different information, but the instructions to review submissions are the same.
2. Click **Triage** to review the submission.

The heading shows the contact’s name, if entered as part of the invitation, and number of items that need to be triaged.

This information, along with the upload date, is also shown on the right side of the page.

![Triage Interface]

Click the More info link below the file to see additional information about the file. The information shown depends on type of file.

3. Review all the items in the submission.

   - Click the checkmark under the file to accept it. The file is marked as accepted and the Evidence Status changes to Active.

   - Click the X under the file to decline it. The file is marked as declined.

     If your agency has a custom retention period for declined evidence, that retention period is used to determine how long the evidence is retained. Otherwise the declined evidence uses the retention period for the associated category to determine when the evidence is queued for deletion.

   - You can accept or decline all remaining files in the submission by clicking **Accept Remaining** or **Decline Remaining**. The number shown in parenthesis on the buttons is the number of files that have not already been accepted or declined.

4. Click **Done**, for individual invites, or **Next Submission**, for public portals.

   If you exit before accepting or rejecting all the items, you can return to the Submission Details Page later from the Portal Details Page.
Searching for Axon Citizen Evidence in Evidence.com

You can use the evidence search pages — All Evidence, My Evidence, or Shared Evidence - to find evidence submitted through Axon Citizen.

1. Enter **AXONCitizen** in the Tag search filter. This shows all evidence submissions from Axon Citizen.

   ![AXONCitizen Tag](image)

   If needed, you can use User or Group, Date, and Category filters to narrow the search results.

   To find evidence submissions that still needs to be triaged, you can select **Triage Pending** in the Status Advanced Search filter to show items that have not been accepted. To find submissions that are declined, you can select the **Declined** status filter.

   **Note:** By default, the Status Advanced Search filter is set to Active and will not show evidence submissions with a Triage Pending status.

2. Click on the evidence **Title** to go to the Evidence Detail Page.

Additional Information on Citizen Evidence Detail Pages

In addition to the usual information on the Evidence Detail page, the following additional information is included for evidence submitted through Axon Citizen.

**Title**

The default Evidence Title includes Axon Citizen, the file type, and the name and phone number of the contact that submitted the evidence. If the contact's information is not stored on Evidence.com, then the contact name is listed as Unidentified and the phone number is not included.

The examples below show the Title where the contact information is stored (left) and not stored (right).

**Note:** Title information can be edited to change the default information.

![Axon Citizen Photo](image)  ![Axon Citizen Photo](image)

**Recorded On and Uploaded On Dates**
Some devices do not include the recorded/created on date for a file when it is submitted to Axon Citizen. In these situations, the Recorded On date is set to the time the file is received in Evidence.com, so the Recorded On and Uploaded On dates will be the same.

**Citizen Metadata**

This section is added to the right-side of the Evidence Detail page and shows the status, contact information, and caption applied by the contact. If the contact's information is not stored on Evidence.com, then the contact information is listed as **Not provided**.

Once a submission is accepted, the **Triaged By** line shows the name and Badge ID for the user that accepted the evidence. Before a submission is triaged, the **Triaged By** line is hidden and **Status** is Pending Triage. When Auto-Accept Submissions is enabled for your agency, the **Triaged By** line is hidden and the **Status** is Auto-Accepted for any individual invite submissions.

**Note:** For evidence that was accepted prior to the September 2018 release, the **Triaged By** line is hidden and the **Status** is Accepted.

The examples below show Citizen Metadata where the contact information is stored (left) and not stored (right).

<table>
<thead>
<tr>
<th>CITIZEN METADATA</th>
<th>CITIZEN METADATA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status: Accepted</td>
<td>Status: Accepted</td>
</tr>
<tr>
<td>Name: Jones, Don</td>
<td>Name: Not provided</td>
</tr>
<tr>
<td>DOB: Jul 4, 1982</td>
<td>DOB: Not provided</td>
</tr>
<tr>
<td>Phone: +12069151016</td>
<td>Phone: Not provided</td>
</tr>
<tr>
<td>Caption: “Just before accident”</td>
<td>Caption: Not provided</td>
</tr>
</tbody>
</table>

**Axon Citizen Audit Trail Information**

The information shown audit trail for Axon Citizen evidence varies depending on if the community member's information is provided. If your agency requires contact information to be stored or if the user sending the invitation selects the store contact information option, then the required community member information, including phone number or email address, is shown in the audit trail. If contact information is not stored, then the audit trail shows the community member information as **Unidentified (name not provided)** and the phone number or email address is not included.
The first example below shows an audit trail entry where the contact information is stored and the second where the contact information is not stored.

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>27 Feb 2018</td>
<td>08:21:04 (-08:00)</td>
<td>Community Member: John T Doe Phone Number: +12060364541</td>
</tr>
<tr>
<td>4</td>
<td>20 Feb 2018</td>
<td>02:08:08 (-08:00)</td>
<td>Community Member: Unidentified (name not provided)</td>
</tr>
</tbody>
</table>

### What Community Members See

#### Public Portal

This section provides an overview of what community members see and how they interact with public portals.

**Note:** For agencies that have French set as their default language in Evidence.com, the Axon Citizen upload screen text, Terms of Use, and Privacy Policy information will also appear in French.

The community member clicks the agency provided link and is taken to the portal welcome page. The community member clicks **Submit Evidence**, enters their information, and then clicks **Send Link** to receive a private link. The private link for submissions expires after 3 days.
After clicking **Send Link**, the citizen receives the text message on their phone with the private link. Tapping the link takes them to a website where they can upload files.

From the upload screen, the community member can add files for uploading. They also have the option of adding a caption for each file. More files can be added by tapping **Add more**. Each submission is limited to a maximum of 16 files, with a maximum size of 2 GB per file and a total submission size of 10 GB.

After the community member has added all their files and the files are uploaded to the website, they tap **Submit** to transfer the files to your agency's Evidence.com account and then can close their browser.

**Individual Invite – Phone**

This section provides an overview of what a community member sees and how they interact with an individual invite sent to their phone.

- After the invite is sent, the community member receives the text message on their phone with the private link. Tapping the link takes them to a website where they can upload files.
• The first screen welcomes them. Tapping **Continue** takes them to the upload screen.

• From the upload screen, the community member can add files for uploading. They also have the option of adding a caption for each file. More files can be added by tapping **Add Files**. Each submission is limited to a maximum of 16 files, with a maximum size of 60 GB per file and a total submission size of 200 GB.
After the community member has added all their files and the files are uploaded to the website, they tap **Submit** to transfer the files to your agency's Evidence.com account and then can close their browser.

**Individual Invite - Email**

This section provides an overview of what a community member sees and how they interact with an individual invite sent to their email.
• After the invite is sent, the citizen receives the email message with the private link. Clicking the link or **Get Started** takes them to a website where they can upload files.

![SB-PRO-QA](https://example.com/sb-pro-qa.png)

**SB-PRO-QA**

Evidence Submission Request

Dear Don,

Thank you for assisting the SB-PRO-QA.

Click the link below to go to a secure webpage and upload your files.

https://sb-pro-qa.evidence.com/axon/citizen/share/c0pzb5wT5sf5c8lh7xiu7ghAEZvya2nZOFn_s2yYvr

Sincerely,
The SB-PRO-QA

[GET STARTED]

• From the upload page, the community member can add files for uploading. They also have the option of adding a caption for each file. More files can be added by clicking **Choose Files**. Each submission is limited to a maximum of 16 files, with a maximum size of 60 GB per file and a total submission size of 200 GB.

![Upload Page](https://example.com/upload.png)

• After the community member has added all their files and the files are uploaded to the website, they click **Submit** to transfer the files to your agency's Evidence.com account and then can close their browser.
Thank you

Your files have been submitted
Evidence Management

For administrators and users allowed the relevant Evidence Management permissions, Evidence.com provides many features for working with evidence files.

Import Evidence

Administrators and users who are allowed the Upload External Files permission can import evidence files into your Evidence.com agency. The user who uploads evidence files becomes the owner of the evidence.

You can use this feature to import evidence that was not recorded on Axon devices, such as pictures taken with your smartphone and saved on your computer.

When you import an evidence file, Evidence.com classifies the file by its file type by the file extension, such as .jpg, .mp3, and .docx. You can filter evidence searches by file type. If Evidence.com does not recognize a file extension, it classifies the file as “Other”.

The maximum file size is 2 Gigabytes.

1. On the menu bar, click Evidence and then click Import Evidence.

   The Import Evidence page appears.
2. Add the files that you want to import, using either of the following methods:
   - Find the files on your computer and then drag and drop the files onto the Import Evidence page.
   - Click Select Files and then use the dialog box to find and select the files on your computer.

3. For each file that you added, provide the following information:

<table>
<thead>
<tr>
<th>Information</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>A meaningful name for the evidence. If you omit the title, Evidence.com assigns the file name as the title.</td>
</tr>
<tr>
<td>ID</td>
<td>It is recommended that you assign evidence the same ID as the case that the evidence is associated with. After you import evidence, you can easily add it to the case.</td>
</tr>
<tr>
<td>Category</td>
<td>Determines the retention period for evidence that is not assigned to an active case. For sensitive evidence, restricted categories provide additional, permission-based control of who can view the evidence.</td>
</tr>
</tbody>
</table>

**Note:** Although it is recommended that you add the title, ID, and category now, Evidence.com enables you to add this information after importing the evidence.

4. Click **Upload Evidence**.

   Evidence.com begins uploading the evidence files. When Evidence.com has successfully uploaded a file, the Progress column shows “Upload Complete”.

5. If you want to view evidence that you uploaded, under Progress, click **Upload Complete**.

6. When you have finished uploading evidence files, close the Import Evidence page.

---

**Evidence Search — All Evidence, My Evidence, and Shared Evidence**

Evidence.com provides a search feature to help you find the evidence you need. In the Evidence area, you can use any of three evidence search pages:

- **All Evidence** — Finds all evidence, including evidence that you do not have permission to view.
- **My Evidence** — Finds evidence that you own or uploaded. The User or Group filter is automatically set to your name.
- **Shared Evidence** — Finds evidence that has been shared with you by the evidence owner.
1. On the menu bar, click **Evidence**.

The All Evidence page lists all evidence, sorted by the most recently recorded evidence.

2. Search for the evidence that you need. The following table provides steps for search-related tasks.

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>View evidence</td>
<td>In search results, click the title of the evidence that you want to view.</td>
</tr>
<tr>
<td>Find evidence that you own</td>
<td>Click <strong>My Evidence</strong>.</td>
</tr>
<tr>
<td>Find evidence that is shared with you</td>
<td>Click <strong>Shared Evidence</strong>.</td>
</tr>
</tbody>
</table>
| Change search results       | 1. Update the evidence search filters. For more information, see Evidence Search Filters.  
                               | 2. Click **Search**.                                                 |
| Sort search results         | Use the **Sort By** list to select **ID, Title, Uploaded Date, or Recorded Date** and click **Sort Order** to change order.  
                               | When in Table view, click the column headings for **ID, Title, Uploaded Date, or Recorded Date**. |
| Switch between page layout options (table, detailed, or gallery) | On the **Page Layout** list, click the layout you want.              |

For information about the actions you can take from evidence search results, see [Working with Evidence Search Results](#).
Evidence Search Filters

Evidence search filters help you limit search results to the evidence files that you want to see. Evidence.com includes in search results only the evidence files that match all the search filters that you set.

Search results are updated as you enter information into the search filters.

**Basic Search Filters:** These are always visible.

- **ID** — Limits search results to evidence whose ID includes the characters you enter in the ID box. For more information, see Text Search Details. You can also enter “None” as the search term to find evidence that does not have an ID.

- **Title** — Limits search results to evidence whose title includes the characters you enter in the Title box. For more information, see Text Search Details.

- **User or Group** — Limits search results to evidence owned by, recorded by, or uploaded by the group the user specified. To specify a user or group name, click in the box, start typing the name of the user or group, wait for Evidence.com to show the matching groups, and then click the group you want.

  On the My Evidence page, the User or Group filter is set to your name by default.

- **Date** — Limits search results by either the recorded on, uploaded on, or deleted on date and time for the evidence. You must specify a date and time range by using the Start and End boxes, otherwise the search is not limited by date range. Search results are inclusive of the dates specified.

  - **Start** — The start of the date and time range. If the Start box is empty, the date range begins with the earliest possible date.

  - **End** — The end of the date and time range. If the End box is empty, the date range ends with today.

- **Category** — Limits search results to evidence that is assigned to the category that you select. Categories determine the retention period of evidence assigned to them. By default, search results include evidence assigned to any category, including uncategorized evidence. You can also enter “None” as the search term to find evidence that does not have a category.

- **Tag** — Limits search results to evidence whose tags includes the characters you enter in the Tag box. For more information, see Text Search Details. You can also enter “None” as the search term to find evidence that does not have a tag. In addition to the tags applied by your agency, there are three Axon generated tags that are automatically applied to certain evidence files; AXONClip is applied to evidence that has been extracted from a
clip, AXONRedaction is applied to evidence that has been extracted from a redaction, and AXONCitizen is applied to evidence that was submitted through Axon Citizen.

**Advanced Search Filters:** Click Show Advanced Search to show these additional search filters.

- **File Type** — Limits search results to the file type selected. By default, search results include all file types.

- **Status** — Limits search results to evidence whose status matches the status selected. By default, evidence searches are limited to evidence with a status of Active.

- **User Association** — Limits search results to evidence that was uploaded by the specified user OR is owned by the specified user. Selecting both will show evidence that was uploaded or is owned by the specified user.

- **Restricted** — Limits search results to evidence that has been restricted.

- **Date Type** — Limits Date search results to the selected date type.

- **Flag** — Limits search results to evidence whose flag status matches the flag status selected.

- **Source** — Limits search results to evidence from the selected type of device that produced the evidence file.

  The Body Worn Cameras option applies to all Axon Body Worn Cameras. The Fleet option applies to both Axon Fleet 2 and Axon Fleet. Evidence that has been extracted or redacted is included in the Other option.

- **Device Serial** — Limits search results to evidence from a particular device.

- **Vehicle ID** — Limits search results to evidence from a particular vehicle. Note that this field only appears if your agency uses Axon Fleet and a vehicle has been added to your account with the Vehicle Configuration.

- **Mount Orientation** — Limits search results to front or back Axon Fleet 2 or Axon Fleet cameras.

**Text Search Details**

The ID, Title, and Tag filters provide advanced text matching capability for evidence searches.

- You can enter letters, numbers, and the special characters: comma (,), dash (-), opening parentheses (()), closing parentheses ()), slash (/), and backslash (\).
• The text you enter can be a full or partial match of the data you are filtering. For example, if you enter 21 in the ID box, then any evidence with 21 in any portion of the ID is included in search results.

• You can search for more than one text string in a single filter by adding a space between the strings. This provides AND search functionality of the data you are filtering. For example, if you enter 12- 34 in the ID box, search results include any evidence with both 12- and 34 in the ID, such as 12-3456 and 12-7348.

• The order of text strings is irrelevant. For example, if you enter 78 21 in the ID box, search results include evidence with the ID 21378 and 17821.

• Capitalization for letter characters is irrelevant. For example, if you enter REDACT in the Title box, search results include evidence with the Title REDACT, redact, and redaction.

**Evidence Search View Type**

Search results can be shown in table view (default) or gallery view. The table view shows the results as a list, while the gallery view shows thumbnail images for the results. Examples of the table and gallery views are shown below.
Working with Evidence Search Results

On evidence search pages — All Evidence, My Evidence, or Shared Evidence — you can take the actions described in this section.

View Evidence

You can view evidence listed in evidence search results if any of the following are true:

- You own the evidence.
- The owner of the evidence has shared it with you.
- Your user role allows you to view all evidence.
- You are a monitor of a group that the evidence owner is a member of.
- You are an administrator.

1. Search for the evidence you want to view.
2. In the search results, click the title of the evidence.

   The Evidence Detail page opens.

   For information about the actions you can take from the Evidence Detail page, see Working with Any Evidence and Working with Video and Audio Evidence.
Request Access

On the All Evidence page, the results can include evidence that you do not own and that you do not have permission to view.

1. On the menu bar, click Evidence.

2. Search for the evidence that you want to view.

3. For an evidence file that you want the owner to share with you, under Status, click Request Access.

<table>
<thead>
<tr>
<th>ID</th>
<th>Title</th>
<th>Owner</th>
<th>Uploaded On</th>
<th>Recorded On</th>
<th>Category</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>45-1555</td>
<td>1</td>
<td>Manning, Harlan (57414)</td>
<td>21 Feb 2017 17:51:23</td>
<td>21 Feb 2017 17:48:41</td>
<td>Os</td>
<td>15 Year; 00000-China</td>
</tr>
<tr>
<td>Add</td>
<td>AICN Body 2 Video 201...</td>
<td>Manning, Harlan (57414)</td>
<td>21 Feb 2017 17:48:18</td>
<td>21 Feb 2017 17:39:24</td>
<td>Os</td>
<td>00000-Show</td>
</tr>
</tbody>
</table>

A message dialog box appears.

4. If you want to include a message to the evidence owner, type it in the Message box.

5. Click Send.

6. On the notification message box, click OK.

   Evidence.com sends the owner a notification email about your request.
After the owner grants you access, Evidence.com sends you a notification email. You can access the evidence from the All Evidence page and the Shared Evidence page.

**Adding Users and Groups to the Inside My Agency Access List from the Evidence Search Page**

From the evidence search page, you can add users and groups to the access list for multiple evidence files at the same time. You can also replace the current access list with a different one.

**Note:** This procedure can also be used to add users and groups to the access list for evidence that has been restricted.

1. Search for the evidence files you want to work with.

2. In the search results, select the check box to the left of the evidence ID for each evidence file that you want to grant access to.

3. Above the search results, click **Manage Access** and select **Inside My Agency**.

4. From the **Access Level** list, select the access level for the user or group.
If **Role** is selected, the actions a user can take with the evidence depends on the permissions associated with their assigned role.

If **View** is selected, the user can only view the evidence.

5. From the **Duration** list, select the period of time the user or group can access the evidence.

The default value is Until Removed, which means access to the evidence is granted until the user or group is removed from the access list.

6. Select how the access lists for the selected evidence files are affected:

   - Select **Add Names Below to Access List** to add the selected users or groups to the current access list.

   - Select **Replace Access List with Names Below** to replace the users and groups currently on the access list with the list of users and groups added below.

     If this option is selected, only users and groups added below will be on the access list for the selected evidence files. All other users and groups will be removed from the access list.

7. In the **User or Group** field, start typing the name, badge ID, or email address of the user or the name of the group. Evidence.com shows a list of matching users or groups as you enter the information. Select the user or group you want to add to the access list.

   **Note:** If you incorrectly add a user or group to the list, you can remove them by clicking the (remove) icon and then clicking **Remove**.
8. Repeat step 7 to add other users and groups.

9. Click **Add** or, if **Replace Access List with Names Below** was selected, **Replace**.

10. A dialog box showing access was granted is displayed. Click **Close** to continue.

An email is sent to each user informing them that they have been added to the access list for the selected evidence files.

### Adding Users and Groups to an Outside My Agency Access List from the Evidence Search Page

This option allows you to add users and groups to an external access list for multiple evidence files at the same time.

The external access list allows you to share evidence with users and groups that are outside your agency. You should use external access list when you need to require that evidence is only available to users who sign in to Evidence.com. You can control whether users you share evidence with can view the evidence, download the evidence, view the audit trail of evidence, and share the evidence with others.

The external access list grants each user and group the same permissions to the evidence. If you need to grant different permissions to different users or groups, perform this procedure once for each set of users or groups to whom you want to grant the same permissions.

Removing users or groups from an access list and changing sharing expiration date cannot be done in bulk. If you need to perform these tasks, you must do it for each evidence file. For more information, see [Modifying and Removing User and Groups from External Access Lists](#).

1. Search for the evidence files you want to work with.

2. In the search results, select the check box to the left of the evidence ID for each evidence file that you want to grant access to.

3. Above the search results, click **Manage Access** and select **Outside My Agency**.

The Manage access outside my agency dialog box displays.
4. Under **Add Name to External Access List**.

![Manage access outside my agency](image)

5. In the **Send an Email with a Link to this Evidence** field, add the users and groups with whom you want to share the evidence, as follows:

   - For a user or group in a partner agency, start typing the name, wait for Evidence.com to show the matching users and groups, and then click the user or group you want to add to the access list. You can also type the user badge ID or email address.

   The user or group you selected appears below the field.

6. In the **Permissions** section, select the check boxes for the permissions that you want to give to the individual users and group users you are adding to the access list.

   - View — User can view the evidence.
   - Download — User can download a copy of the evidence to their hard drive.
   - View Audit Trail — User can view the audit trail.
   - Post Notes — User can add notes to the evidence.

7. Select the **Allow Users to Re-Share** option for the selected evidence.
• Never — User cannot share the evidence.
• Reshare Download — User can forward the permission to download to other users.
• Reshare All — User can forward all of their permissions to other users.

8. In the **Duration** box, type the number of days that the evidence is to be available to the users.

9. Click **Add** and then, on the confirmation message box, click **OK**.

Evidence.com emails each user you added to the access list, notifying them that the evidence is available to them.

### Providing Evidence Outside My Agency by Unauthenticated Download Link from the Evidence Search Page

Sending download link makes the evidence available through a web link, or URL, for downloading a ZIP file of the evidence from Evidence.com — **without requiring the person downloading the evidence to sign in to Evidence.com.**

Sending a download link allows uncontrolled access to the ZIP file of evidence that it links to. By default, evidence sent by download link is only available for download for 3 days. It is recommended that you keep the duration as short as possible.

1. Search for the evidence files you want to work with.

2. In the search results, select the check box to the left of the evidence ID for each evidence file that you want to grant access to.

3. Above the search results, click **Manage Access** and select **Outside My Agency**.

4. The Manage access outside my agency dialog box displays.
5. Click **Email a Download Link**.

6. In the **Send an Email with a Link to this Evidence** field, add the users with whom you want to share the evidence, as follows:

   - For a user in your agency or a partner agency, start typing the name of the user, wait for Evidence.com to show the matching users, and then click the user you want. You can also type the user badge ID or email address. The user you selected appears below the field.
   
   - For a user who is not in your agency or a partner agency, type the email address of the user and then press **Enter**.

   After you complete the sharing process, the person receiving the sharing invitation can download the evidence ZIP file.

7. If you want to include audit trails, check the corresponding check box.

8. In the **Duration** box, type the number of days that the evidence is to be available to the users you share the evidence with.

9. Click **Add**.

10. On the notification message box, click **Close**.
Each recipient you specified receives an email that includes the link for downloading the evidence.

Evidence.com makes the shared evidence available for download, until the sharing duration expires.

**Restricting Evidence from the Evidence Search Page**

Evidence files can be restricted by adding a restricted category to the evidence or by manually restricting the evidence.

Restricting an evidence file only allows users that are on the access list or that are assigned to a role with Access Restricted Evidence permission to view the evidence. When searching for evidence files, users can see restricted evidence files in the search results, but cannot view the evidence file.

From the evidence search page, you can add users and groups to the access list and restrict evidence for more than one evidence file at a time. You can also replace the current access list with a different one and restrict the files.

1. Search for the evidence files you want to work with.

2. In the search results, select the check box to the left of the evidence ID for each evidence file that you want to grant access to and restrict.

3. Above the search results, click **Manage Access** and select **Restrict**.
The Restrict access in my agency dialog box displays.

**Note:** If you are not already on the access list, you are automatically added to the list.

4. From the **Access Level** list, select the access level for the user or group.

- If **Role** is selected, the actions a user can take with the evidence depends on the permissions associated with their assigned role.

- If **View** is selected, the user can only view the evidence.

5. From the **Duration** list, select the period of time the user or group can access the evidence.

The default value is Until Removed, which means access to the evidence is granted until the user or group is removed from the access list.

6. Select how the access lists for the selected evidence files are affected:

- Select **Add Names Below to Access List** to add the selected users or groups to the current access list.

- Select **Replace Access List with Names Below** to replace the users and groups currently on the access list with the list of users and groups added below.

If this option is selected, only users and groups added below will be on the access list for the selected evidence files. All other users and groups will be removed from the access list.
7. In the **User or Group** field, start typing the name, badge ID, or email address of the user or the name of the group. Evidence.com shows a list of matching users or groups as you enter the information. Select the user or group you want to add to the access list.

**Note:** If you incorrectly add a user or group to the list, you can remove the user by clicking the ![remove](remove) icon and then clicking **Remove**.

8. Repeat step 7 to add other users and groups.

9. Click **Restrict** or, if **Replace Access List with Names Below** was selected, **Replace and Restrict**.

10. A dialog box showing access was granted is displayed. Click **Close** to continue.

   An email is sent to each user informing them that they have been added to the access list for the selected evidence files.

   **Note:** An email is sent to users that were already on the access list for this evidence informing them that the evidence was restricted, but that they still have access.

### Update ID

You can change the ID assigned to one or more evidence files in search results.

An evidence ID can be up to 24 alphanumeric characters, unless your administrator has configured evidence ID validation that enforces different minimum or maximum ID length.

1. Search for the evidence whose ID you want to update.

2. For each evidence file whose ID you want to update, select the check box to the left of the evidence.

3. Above the search results, click **Update ID**.

   A dialog box appears.

4. In the New ID box, type the ID that you want to assign to all selected evidence and then click **Update**.

5. On the notification message box, click **OK**.

   The search results show the new ID that you assigned to the evidence.

### Add Category to Evidence

You can add a category to one or more evidence files in search results.
A category name can be up to 50 alphanumeric characters.

1. Search for the evidence that you want to add a category to.

2. For each evidence file that you want to add a category to, select the check box to the left of the evidence.

3. Above the search results, click **Add Category**. A dialog box appears.

4. In the New Category list, click the category that you want to add to all selected evidence and then click **Update**.

5. On the notification message box, click **OK**.

   The search results show the category that you assigned to the evidence. If more than one category is assigned to evidence, “Multiple” appears in the Category column for that evidence.

---

**Reassign Evidence**

When you need to change the owner of evidence to another user, you can reassign the evidence from the results of an evidence search.

1. Search for the evidence that you want to reassign to another user.

2. For each evidence file that you want to reassign, select the check box to the left of the evidence.

3. Above the search results, click **Reassign**. A dialog box appears.

4. In the **Reassign To** box, start typing the name of the user you want to assign the evidence to, wait for Evidence.com to show the list of matching users, click the user that you want, and then click **Reassign**.

5. In the confirmation dialog box, click **OK**.

   The search results show that the user you selected is now the evidence owner.

---

**Bulk Video Redaction**

Public disclosure requests can be time consuming, especially when large volumes of videos must be reviewed and potentially redacted. To aid with these large requests, the Bulk Redaction feature allows you to queue video evidence for bulk redaction.
Bulk redaction creates a copy of the original video and applies a blur filter over the entire copied video. It can also remove audio for the duration of that copy as well. The blur over the entire video allows requestors to see what happened in the video without potentially revealing personally identifiable details such as faces, addresses, or license plates. This presents an opportunity for agencies to fulfill the public disclosure request in the least amount of time.

It is recommended that you verify bulk-redacted videos to ensure the proper level of blur is applied prior to releasing the redacted videos.

**Note:** If you need to redact a video more precisely, such as redacting only a portion of each video frame, see Video Evidence Redaction.

1. Search for the video evidence that you want to include in the bulk redaction.

2. For each video evidence file that you want to redact, select the check box to the left of the evidence ID. If you want to redact all evidence shown in search results, select the check box at the top left of the search results.

3. Click **Redact**.

The Bulk Redaction dialog box appears. The number of files selected and estimated download file size is shown in the upper right of the dialog box.

![Bulk Redaction Dialog Box](image)

4. Under **Download Format**, select the file format you want to use when downloading the completed redacted video files:
   - ZIP — Evidence.com includes the redacted videos in a ZIP file.
   - ISO — Evidence.com includes the redacted videos in an ISO image, which can be used to create a CD-ROM or DVD.

5. Under **Blur Level**, click the degree of blurring that you want Evidence.com to apply to the video files.
6. Select If you want Evidence.com to remove all audio from the redacted video files.

   If you want the original audio of all video files to be preserved in the redacted video files, set the **Redact Audio** switch to **OFF**.

7. Click **Redact**.

8. On the confirmation message box, click **OK**.

   When bulk redaction service is complete, Evidence.com sends you an email with a download link for the ISO or ZIP file.

9. In the notification email, click the download link.

   A web browser opens your Evidence.com agency.

10. If the sign-in page appears, enter your Evidence.com credentials and click **Sign In**.

   Evidence.com opens or downloads the bulk-redacted video evidence file. The exact behavior depends on the browser you use and its download settings for files.

---

**Bulk Download Evidence**

Users who are allowed the Download permission for evidence can download multiple evidence files at a time. After selecting files for download, the user receives an email with a download link to a single file containing all of their requested evidence. Evidence.com supports the following file types for the download file:

- **ZIP** — Evidence.com includes the selected evidence files in a ZIP file.
- **ISO** — Evidence.com includes the selected evidence files in an ISO image, which can be used to create a CD-ROM or DVD.

**Note:** We have noted a system issue where large bulk download requests were failing to complete. This issue should not affect most customers. But as a short-term fix, we are temporarily limiting the size of bulk downloads to a total of 10 GB per download while we determine a long-term solution. Additionally, if a user selects evidence exceeding 10 GB, a message warning the user that the download exceeds the allowed limit is shown.

1. Search for the evidence that you want to download.

2. For each evidence file that you want to include in the download, select the check box to the left of the evidence ID. If you want to include all evidence shown in search results, select the check box at the top left of the search results.
3. Click **Download**.

The Bulk Download dialog box lists all the files you selected. At the bottom of the dialog box are options for including audit trails, download file type, and the Download button.

4. Select the **Download Format** to set the file type that you want as the download file.

5. If you want to include audit trails for the selected evidence files, click the **Audit Trail** check box.

6. Click **Download**. If the Download button is not visible, scroll down to the bottom of the dialog box.

   When the files are ready to download, you receive an email with a link to download the ZIP or ISO file.
7. In the notification email, click the download link.

A web browser opens your Evidence.com agency.

8. If the sign-in page appears, enter your Evidence.com credentials and click **Sign In**.

Evidence.com opens or downloads the file. The exact behavior depends on the browser you use and its download settings for files.

### Download Speed Information

Files on Evidence.com will download at different rates. Evidence.com does not throttle file downloads. The speed of your download depends on file size and your Internet connection speed.

File sizes on Evidence.com will vary, depending on a number of factors, such as recording quality and duration. The size of an evidence file can be found in the Metadata section of the evidence view.

Your Internet Service Provider can help you determine your specific download speed or you can check your speed with an online Internet Speed Test tool. If you are seeing issues where your download times are significantly different than the estimated download time, you should check with your IT organization for any potential issues with your network. If you require additional assistance, contact Technical Support via support@axon.com or at 800-978-2737 ext 2 or +1 480-463-2170.

The table below provides estimated download times for different files sizes and download speed.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>25 MB</td>
<td>10 seconds</td>
<td>13 seconds</td>
<td>20 seconds</td>
<td>30 seconds</td>
<td>1.75 minutes</td>
</tr>
<tr>
<td>50 MB</td>
<td>17 seconds</td>
<td>30 seconds</td>
<td>40 seconds</td>
<td>50 seconds</td>
<td>3.5 minutes</td>
</tr>
<tr>
<td>100 MB</td>
<td>30 seconds</td>
<td>1 minute</td>
<td>1.5 minutes</td>
<td>1.75 minutes</td>
<td>7 minutes</td>
</tr>
<tr>
<td>250 MB</td>
<td>1.5 minutes</td>
<td>2.5 minutes</td>
<td>3.5 minutes</td>
<td>4.5 minutes</td>
<td>17.5 minutes</td>
</tr>
</tbody>
</table>

### Delete Evidence

You can delete evidence files that are listed in evidence search results. Evidence that you delete is added to a deletion queue for 7 days. This helps prevent deleting evidence unintentionally.
1. Search for the evidence that you want to delete.

2. For each evidence file that you want to delete, select the check box to the left of the evidence.

3. Above the search results, click **Delete**.

   A confirmation dialog box appears.

4. Click **OK**.

   A comment dialog box appears.

5. If you want to make a comment about the deletion, type it in the box provided.

6. Click **OK**.

7. On the notification message box, click **OK**.

   In the search results, the status of the evidence changes to “Queued for Deletion”.

### Restore Evidence

From evidence search results, you can restore evidence that has a status of Queued for Deletion. Restoring evidence removes it from the deletion queue.

**Note:** When evidence that is queued for deletion is restored, if the evidence is assigned a category that has a retention period, the evidence's new deletion date is set 30 days from the current date, regardless of the categories retention period. If the evidence is assigned to a category that does not have a retention period, then no deletion date is set for the evidence.

1. Search for the evidence that you want to restore. Ensure that, in the **Status** list, you click **Queued for Deletion**.

2. For each evidence file that you want to restore, select the check box to the left of the evidence.

3. Above the search result, click **Restore**.

4. On the confirmation message box, click **OK**.

5. On the notification message box, click **OK**.

   In the search results, the status of the evidence does not change.

6. If you want to confirm that the evidence status has changed to Active, search for the evidence again.
Export Evidence Search Results

**Note:** The Reporting feature includes several evidence-related reports. For more information, see Reporting.

You can export the results of an evidence search as a list in PDF, Excel, text, or CSV format.

**Note:** When evidence search results are exported in Microsoft Excel or CSV format, the Device Assignee First Name and Last Name are split into separate columns and a Badge ID column is included.

If the search results contain more than 500 evidence files, Evidence.com provides the list in 500-file segments and asks you to confirm the download of the next segment.

1. Search for evidence and refine the search until the search results represent the evidence list that you want to export.

2. Above the search results, click **Export**.

3. In the **Select Format** list, click the file format that you want for the exported evidence list and then, on the message box, click **Export**.

   The evidence list downloads in the format that you specified.

   If the evidence search results contain more than 500 evidence files, only the first 500 files are included in the downloaded list and Evidence.com displays a dialog box for downloading the next 500 files in the search results.

4. If you want to export evidence lists for additional evidence, click **OK** each time the dialog box appears.

   The evidence lists download in a separate evidence list file for each 500-file segment of the search results.

Working with Any Evidence

This section describes the actions available on the Evidence Detail page for all evidence file types.

Actions available for video and audio files only are described in Working with Video and Audio Evidence.
Adding Users and Groups to the Inside My Agency Access List from the Evidence Detail Page

On the Evidence Detail page, the Manage Evidence Access section shows the number of users and groups that have been added to the access list for the evidence and if the evidence is restricted.

From the Manage Evidence Access section you can add users and groups to the access list for an evidence file. If you want to add users and groups to the access list for more than one evidence file at a time, use the process for adding access from the evidence search page.

Note: This procedure can also be used to add users and groups to the access list for evidence that has been restricted.

1. On the Evidence Detail page, under Manage Evidence Access, click Inside My Agency.

The Manage Access page appears.

2. In the User or Group field, start typing the name, badge ID, or email address of the user or the name of the group. Evidence.com shows a list of matching users and groups as you enter the information. Select the user or group you want to add to the access list.
You can add multiple users and groups if they will have the same access duration and access level.

3. From the **Access Level** list, select the access level.

   - If **Role** is selected, the actions a user can take with the evidence depends on the permissions associated with their assigned role.
   
   - If **View** is selected, the user can only view the evidence.
4. From the **Duration** list, select the period of time the user can access the evidence.

The default value is Until Removed, which means the user can access the evidence until they are removed from the access list.

5. Click **Add**.

The user information is added to the list and an email is sent to the user informing them that they have been added to the access list for the evidence.

6. Repeat steps 2 through 5 to add other users.

7. After all users are added, click the (back) button to return to the Evidence Detail page.

---

**Modifying Inside My Agency Access Information**

You can modify the access duration and access level for users from the Evidence Detail page.

**Note:** This procedure can be used to modify access information for evidence that has been restricted.

1. On the Evidence Detail page, under Manage Evidence Access, click **Inside My Agency**.
The Manage Access page appears.

2. In the access list, click the 🍀 (edit) icon on the same line as the user or group you want to modify.
3. Select the access level and duration as needed.

![MANAGE ACCESS](image)

4. Click Save.

5. Repeat steps 2 through 4 for other users or groups in the list.

6. When you have finished modifying access information, click the (back) button to return to the Evidence Detail page.

Removing Users and Groups from the Inside My Agency Access List

Users can only be removed from the access list for an evidence file from the Evidence Detail page.

Note: This procedure can be used to remove users from the access list for evidence that has been restricted.
1. On the Evidence Detail page, under Manage Evidence Access, click **Inside My Agency**.

![Evidence Detail Page](image)

The Manage Access page appears.

2. In the access list, click the (remove) icon and then click **Remove**.

   The user or group is removed from the list and an email is sent to the users informing them that they have been removed from the access list for the evidence.

3. Repeat step 2 to remove other users from the list.

4. When you have finished removing users, click the (back) button to return to the Evidence Detail page.

### Adding Users and Groups to the Outside My Agency Access List

On the Evidence Detail page, the Manage Evidence Access section shows the number of users and groups that have been added to the access list for the evidence and if the evidence is restricted.

From the Manage Evidence Access section you can add users and groups to the access list for an evidence file. If you want to add users and groups to the access list for more than one evidence file at a time, use the process for [adding access from the evidence search page](#).
1. On the Evidence Detail page, under Manage Evidence Access, click **Outside My Agency**.

The Access outside my agency page appears.

2. In the **User or Group** field, start typing the name, badge ID, or email address of the user or the name of the group. Evidence.com shows a list of matching users and groups as you enter the information. Select the user or group you want to add to the access list.

You can add multiple users and groups if they will have the same access duration and access permissions.
3. In the **Permissions** section, select the check boxes for the permissions that you want to give to the users you are sharing with.

![Permissions section](image)

- Download — User can download a copy of the evidence to their hard drive.
- View Audit Trail — User can view the audit trail.
- Add Notes — User can add notes to the evidence.

4. Select the **Allow Partner Agencies to Re-Share** option for the selected evidence.

- Never — User cannot share the evidence.
- Reshare Download — User can forward the permission to download to other users.
- Reshare All — User can forward all of their permissions to other users.

5. In the **Duration** box, type the number of days that the evidence is to be available to the users you share the evidence with.

6. Click **Add**.

   Evidence.com emails each user who you shared the evidence with, notifying them that the evidence is available to them.

7. To add a user or group with different permissions or duration, click **Add New** and repeat steps 2 through 6 to add other users and groups.
8. After all users and groups are added, click the ‹ (back) button to return to the Evidence Detail page.

**Modifying and Removing Users and Groups from Outside My Agency Access Lists**

You can modify the access permissions and access duration for users and groups from the Evidence Detail page.

1. On the Evidence Detail page, under Manage Evidence Access, click **Outside My Agency**.

The Access outside my agency page appears.
2. To modify user or group information, click the ✉️ (edit) icon on the same line as the user or group you want to modify.

Modify the permissions, reshare, and duration information as needed.

3. Click Save.

4. Repeat steps 2 through 4 for other users or groups in the list.

5. To remove a user or group from the outside my agency access list, click the 🗑️ (remove) icon and then click Remove.
The user or group information is removed to the list and an email is sent to the users informing them that they have been removed from the access list for the evidence.

6. Repeat step 5 to remove other users or groups from the list.

7. When you have finished modifying access information, click the (back) button to return to the Evidence Detail page.

Restricting Evidence from the Evidence Detail Page

Evidence files can be restricted by adding a restricted category to the evidence or by manually restricting the evidence.

Restricting an evidence file only allows users that are on the access list or that are assigned to a role with Access Restricted Evidence permission to view the evidence. When searching for evidence files, users can see restricted evidence files in the search results, but cannot view the evidence file.

On the Evidence Detail page, the Manage Evidence Access section shows the number of users that have been added to the access list for the evidence and if the evidence is restricted.

From the Manage Evidence Access section you can add users to the access list for an evidence file and restrict the evidence. If you want to add users to the access list and restrict evidence for more than one evidence file at a time, use the process for restricting evidence from the evidence search page.

1. On the Evidence Detail page, under Manage Evidence Access, click Inside My Agency.
The Manage Access page appears.

**Note:** Steps 2 and 3 can be done in any order. By doing step 2 first, the user will only get an email saying they were added to the access list for the evidence. If you do step 3 first, the users will get an email saying they were added to the access list and then get a second email when the evidence is restricted saying the evidence was restricted.

2. **Click the Restrict switch.**

The system asks you to confirm that you want to restrict the evidence.

![Confirmation dialog]

Click **Restrict** to continue.

**Note:** If you are not already on the access list, you are automatically added to the list. An email is sent to users and groups that were already on the access list for this
Evidence informing them that the evidence was restricted, but that they still have access.

3. In the **Add to Access List** field, start typing the name, badge ID, or email address of the user or the name of the group. Evidence.com shows a list of matching users as you enter the information. Select the user or group you want to add to the access list.

![Add to Access List](image)

You can add multiple users and groups if they will have the same access duration and access level.

4. From the **Access Level** list, select the access level.
   - If **Role** is selected, the actions a user can take with the evidence depends on the permissions associated with their assigned role.
   - If **View** is selected, the user can only view the evidence.
5. From the **Duration** list, select the period of time the user can access the evidence.

The default value is Until Removed, which means the user can access the evidence until they are removed from the access list.

6. Click **Add**.

The user information is added to the list and an email is sent to the user informing them that they have been added to the access list for the evidence.

7. Repeat steps 3 through 6 to add other users.
8. After all users are added, click the (back) button to return to the Evidence Detail page.

**Removing Restriction from Evidence**

Evidence restriction can only be removed from evidence by removing the restriction an evidence file from the Evidence Detail page. Using the restrict switch to remove restriction will override a restricted category, so you don't need to change categorization in order to remove the restriction from the evidence.

9. On the Evidence Detail page, under Manage Evidence Access, click **Inside My Agency**.

![Evidence Detail Page](image)

The Manage Access page appears.

10. Click the **Restrict** switch.

The restriction on the evidence is removed and an email is sent to each user on the access list informing them that the restriction was removed from the evidence file.

11. Click the (back) button to return to the Evidence Detail page.

**Edit Title and ID**

On the Evidence Detail page, the evidence title and ID appear in the upper-left corner.

An evidence ID can be up to 24 alphanumeric characters, unless your administrator has configured evidence ID validation that enforces different minimum or maximum ID length.

An evidence title can be up to 256 alphanumeric characters.

1. To the right of the evidence title, click (edit).
The title and ID become editable.

2. Edit the title and ID, as needed, and then click **Save**.

The Evidence Detail page shows the updated title and ID.

**Edit Recorded Date and Time**

On the Evidence Detail page, the recorded date and time appear in the Metadata section.

1. To the right of **Recorded On**, click **Edit**.

   The Recorded On box becomes editable. A calendar icon and a clock icon appear.

2. Using the methods provided in the following table, edit the date and time as needed.

<table>
<thead>
<tr>
<th>Action</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directly edit the date and</td>
<td>Click the Recorded On box and enter the changes to the date and</td>
</tr>
<tr>
<td>time.</td>
<td>time.</td>
</tr>
<tr>
<td>Change the date.</td>
<td>Click the calendar icon and then use the calendar tool to select the</td>
</tr>
<tr>
<td></td>
<td>date.</td>
</tr>
<tr>
<td>Change the time.</td>
<td>Click the clock icon and then select the closest time to the time that</td>
</tr>
<tr>
<td></td>
<td>you need.</td>
</tr>
</tbody>
</table>

3. After you have finished editing the recorded date and time, click **Save**.

   A confirmation message box shows the new recorded date and time.

   If the change affects the retention period, the message box shows this information, too.

4. On the confirmation message box, click **OK**.

5. On the notification message box, click **OK**.

**Download Evidence File**

On the Evidence Detail page, the Download button appears above the evidence preview.

1. Click **Download**.

   A dialog box shows information about the evidence file.
2. On the dialog box, click **Download**.

The download begins. The exact behavior depends on the browser you use and its download settings. For more information about download speeds, see the Download Speed Information topic.

3. Click **Cancel**.

**Flag or Un-Flag Evidence**

You can flag evidence that you want to find more easily in the future. Evidence searches allow you to filter the search results by the flag status of evidence.

On the Evidence Detail page, the Flag or Unflag button appears above the evidence preview.

- Evidence that is *not* flagged has a Flag button.
- Evidence that is flagged has an Unflag button.

If you want to flag or un-flag the evidence, click **Flag** or **Unflag**, as applicable.

**Add to or Remove Evidence from a Case**

You can add or remove evidence to one or more cases.

On the Evidence Detail page, the Cases area appears on the right side of the page. If the evidence is in any cases currently, the case IDs appear as links.

1. To the right of **Cases**, click **Edit**.

The Add to Case page appears.
2. If you want to add the evidence to a case, in the **Select Case** list, click a case that you want to add the evidence to, and then click **Assign**.

The case that you selected appears under Associated Cases.

3. If you want to remove the evidence from a case, under **Associated Cases**, find the case and then, to the left of the case, click **X**.

4. When you have finished adding or removing the evidence to and from cases, click **Return to My Evidence**.

---

### Reassign Evidence

You can assign evidence to a user. The user to whom you assign evidence becomes the owner of the evidence.

On the Evidence Detail page, the Reassign button appears above the evidence preview.

1. Click **Reassign**.

The Reassign Evidence page appears.

2. In the **Name** box, start typing the name of the user, wait for Evidence.com to show the matching users, and then click the user you want.

3. Click **Reassign**.

4. On the confirmation message box, click **Yes**.

5. On notification message box, click **OK**.

The Evidence Detail page appears.

---

### View Evidence Audit Trail

You can view the audit trail for an evidence file.
On the Evidence Detail page, the Audit Trail button appears above the evidence preview.

1. Click **Audit Trail**.
   A dialog box provides options for viewing the entire audit trail or a portion of the audit trail.

2. If you want to view the whole audit trail, under **View Entire Audit Trail**, click **Submit**.

3. If you want to view a portion of the audit trail, under **View Portion of Audit Trail**, specify a date in either or both the **From** or **To** boxes and click **Submit**.
   Evidence.com opens or downloads a PDF for the evidence audit trail. The exact behavior depends on the browser you use and its download settings for PDF files.

4. Save or view the audit trail PDF as needed.

---

**Delete Evidence**

You can manually initiate the deletion of an evidence file. Evidence that you delete is added to a deletion queue for 7 days. This helps prevent deleting evidence unintentionally.

On the Evidence Detail page, the Delete button appears above the evidence preview.

1. Click **Delete**.

2. On the confirmation message box, click **Okay**.
   A dialog box appears, allowing you to add a comment regarding the evidence deletion.

3. If you want to add a comment, type it in the comment box.

4. Click **Submit**.
   The evidence status changes to “Queued for Deletion”.

---

**Restore Deleted Evidence**

If evidence has a status of Queued for Deletion, you can restore the evidence, which removes it from the deletion queue.

**Note:** When evidence that is queued for deletion is restored, if the evidence is assigned a category that has a retention period, the evidence's new deletion date is set 30 days from the current date, regardless of the categories retention period. If the evidence is assigned to a category that does not have a retention period, then no deletion date is set for the evidence.
On the Evidence Detail page for evidence that has the status of Deleting, the Restore button appears above the evidence preview.

1. Click **Restore**.
2. On the confirmation message box, click **OK**.

The evidence status becomes Active.

### Assign and Un-Assign Categories

For evidence that is not assigned to a case, changing the categories that the evidence is assigned to may change the scheduled deletion date. If the scheduled deletion date has already passed, the evidence is added to the deletion queue.

On the Evidence Detail page, the Categories area appears in the heading below the evidence Title and ID and on the right side of the page. It lists the categories that the evidence is assigned to, if any.

1. If no categories have been added to the evidence, click **Add Category**. Otherwise, to the right of **Categories**, click **(edit)**.

   The Select a category list appears. If the evidence is already assigned to categories, an X appears beside each assigned category.

2. If you want to assign the evidence to a category, in the **Select a category** list, click the category and then click **Save**.

   The category appears at the bottom of the list of assigned categories.

3. If you want to remove the evidence from a category, click the X next to the category.

   The category is removed from the list of assigned categories.

### Add and Remove Tags for Evidence

Tags are labels that you can apply to evidence and cases. Adding tags to evidence can help you find the evidence more easily later. Evidence searches allow you to filter the search results by tags.

On the Evidence Detail page, the Tags area appears on the right side of the page. If any tags exist, they appear as tiles. The following figure shows an example of the Tags area that has one tag named, “McKinley”.

A tag can be up to 256 alphanumeric characters.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Add tag    | 1. Under **Tags**, click in the box.  
               2. Start typing the tag. Evidence.com shows you a list of existing tags that start with the letters you typed.  
               3. If the tag you want to apply appears in the list, click the tag.  
               4. Otherwise, finish typing the tag and then press **Enter**. Evidence.com adds the tag to the evidence. |
| Remove tag | 1. Under **Tags**, find the tag that you want to remove.  
               2. At the left end of tag, click **X**. Evidence.com removes the tag from the evidence. |

**Edit Location**

The location that you specify for evidence determines where the icon representing the evidence appears on evidence maps.

On the Evidence Detail page, the Location area appears near the upper-right corner of the page. If the evidence has location information, a small map shows the evidence location.

**Note:** You cannot edit the location of evidence recorded by GPS. This applies to Axon Fleet cameras and Axon Body 2 or Axon Flex 2 cameras that are paired with Axon View with GPS enabled.

1. To the right of **Location**, click **(edit)**.

   The Edit Location page shows a map.

2. In the **Address** box, type the location address or coordinates. Optionally, you can add a friendly name description for the location.

   When setting location coordinates: Latitude values can be -90.0000 to 90.0000, where the negative value represents South coordinates. Longitude values can be -180.0000 to 180.0000, where the negative value represents West coordinates.
**Example:** Coordinates of 15 degrees North and 30 degrees East would be entered as 15.0000 and 30.000, while 15 degrees South and 30 degrees West would be entered as -15.0000 and -30.000.

3. Click **Save**.

The map shows the location you entered.

**Edit Description**

You can add or edit a description of the evidence.

On the Evidence Detail page, the description appears below the evidence.

1. To the right of **Description**, click 📐 (edit).

   The description text becomes editable.

2. In the **Description** box, type a new description or edit the existing description.

3. Click **Save**.

   Evidence.com saves the description changes.

**Notes and Evidence**

You can post notes about evidence. In addition to the text of the note, Evidence.com shows the author of the note and the date and time that the note was created and updated.

On the Evidence Detail page, the Notes area appears below the evidence and description. If the Also with ID area appears, the Notes area appears below this area.

**Add a Note**

You can post a note to an evidence file.

1. If necessary, scroll down and find the Notes area.

2. In the **Post a Note** box, type the note.

3. Click **Post Note**.

   Under Notes, the new note appears, with your name and the creation date and time.

**Edit a Note**

You can edit notes that have previously been posted to an evidence file.
1. If necessary, scroll down and find the **Notes** area.

2. To the right of the note, click ✍️ (edit).
   
The note text becomes editable.

3. Edit the note text as needed.

4. Click **Update**.
   
The changes to the note appear, with your name and the date and time that the edits occurred.

### Delete a Note

You can delete notes that you have posted.

1. If necessary, scroll down and find the Notes area.

2. To the right of the note, click X.

3. On the confirmation dialog box, click **OKAY**.
   
The note no longer appears on the Evidence Detail page.

### View Evidence with Same ID

If other evidence in your agency has the same ID as the evidence you are viewing, the **Also with ID** area appears below the evidence description. A paginated table of evidence with the same ID shows the title, assignee, and upload date of each evidence file.

If you want to view evidence listed in the table, click the evidence title.

<table>
<thead>
<tr>
<th>ALSO WITH ID</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TITLE</strong></td>
</tr>
<tr>
<td>Backyard</td>
</tr>
<tr>
<td>Location of Fall: East View</td>
</tr>
</tbody>
</table>

### Viewing Video Source Information

For video uploaded from an Axon device managed by your Evidence.com agency, the Evidence Detail page includes a Source section. The serial number and model of the recording device appear in this section.
To view details about the recording device, click the serial number.

**Viewing Document Evidence**

Evidence.com enables users to view the contents of documents that are in PDF format.

**PDF Viewer Controls**

The following figure shows the controls that appear when you view a PDF document.

**PDF Viewer Actions**

The following table provides steps for the actions you can take with the PDF viewer.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page down</td>
<td>Click <img src="arrow.png" alt="Page down" /> or press the down arrow key.</td>
</tr>
</tbody>
</table>
### Playing Video and Audio Evidence

This section describes the actions available on the Evidence Detail page for video and audio evidence files that are in a file type supported by the Evidence.com media player.

**Supported File Types**

Video file types supported by the Evidence.com media player include the types listed in the following table.

<table>
<thead>
<tr>
<th>Video File Extension</th>
<th>Video Mime Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>.avi</td>
<td>video/avi</td>
</tr>
<tr>
<td>.fli</td>
<td>video/x-fli</td>
</tr>
<tr>
<td>.mov</td>
<td>video/quicktime</td>
</tr>
<tr>
<td>.movie</td>
<td>video/x-sgi-movie</td>
</tr>
<tr>
<td>.mpe</td>
<td>video/mpeg</td>
</tr>
<tr>
<td>.mpeg</td>
<td>video/mpeg</td>
</tr>
<tr>
<td>.mpg</td>
<td>video/mpeg</td>
</tr>
<tr>
<td>.qt</td>
<td>video/quicktime</td>
</tr>
<tr>
<td>.m4v</td>
<td>video/x-m4v</td>
</tr>
<tr>
<td>.webm</td>
<td>video/webm</td>
</tr>
<tr>
<td>.ogv</td>
<td>video/ogv</td>
</tr>
<tr>
<td>.mp4</td>
<td>video/mp4</td>
</tr>
<tr>
<td>.wmv</td>
<td>video/x-ms-wmv</td>
</tr>
</tbody>
</table>

The .avi and .m4v file formats are container file formats. Because it is possible for them to contain unsupported media files, it is possible for files in these formats to be valid but unsupported by the media player.
Audio file types supported by the Evidence.com media player include the types listed in the following table.

<table>
<thead>
<tr>
<th>Audio File Extension</th>
<th>Audio Mime Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>.aif</td>
<td>audio/x-aiff</td>
</tr>
<tr>
<td>.aifc</td>
<td>audio/x-aiff</td>
</tr>
<tr>
<td>.aiff</td>
<td>audio/x-aiff</td>
</tr>
<tr>
<td>.au</td>
<td>audio/basic</td>
</tr>
<tr>
<td>.kar</td>
<td>audio/midi</td>
</tr>
<tr>
<td>.mid</td>
<td>audio/midi</td>
</tr>
<tr>
<td>.midi</td>
<td>audio/midi</td>
</tr>
<tr>
<td>.mp2</td>
<td>audio/mpeg</td>
</tr>
<tr>
<td>.mp3</td>
<td>audio/mpeg</td>
</tr>
<tr>
<td>.mpga</td>
<td>audio/mpeg</td>
</tr>
<tr>
<td>.ra</td>
<td>audio/x-realaudio</td>
</tr>
<tr>
<td>.ram</td>
<td>audio/x-pn-realaudio</td>
</tr>
<tr>
<td>.rm</td>
<td>audio/x-pn-realaudio</td>
</tr>
<tr>
<td>.rpm</td>
<td>audio/x-pn-realaudio-plugin</td>
</tr>
<tr>
<td>.snd</td>
<td>audio/basic</td>
</tr>
<tr>
<td>.tsi</td>
<td>audio/TSP-audio</td>
</tr>
<tr>
<td>.wav</td>
<td>audio/x-wav</td>
</tr>
<tr>
<td>.wma</td>
<td>audio/x-ms-wma</td>
</tr>
</tbody>
</table>

For actions available for all file types, regardless of media player support, see Working with Any Evidence.

**Internet Connection Speed Recommendations**

For the best video playback experience, we recommend that your Internet connection support the speeds listed in the following table:

<table>
<thead>
<tr>
<th>Resolution</th>
<th>Recommended Minimum Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>480p</td>
<td>3 Megabits per second</td>
</tr>
<tr>
<td>720p</td>
<td>6 Megabits per second</td>
</tr>
<tr>
<td>1080p</td>
<td>10 Megabits per second</td>
</tr>
</tbody>
</table>

If your connection is slower than necessary to provide good video playback, you may experience pauses during playback.
Media Player Controls

The Evidence.com media player enables you to play audio and video evidence files that are in supported file types.

The following figure shows the media player controls that appear when the player is paused. Additionally, in the following figure, the sound is not muted.

Available Controls — Player Paused, Sound Unmuted

<table>
<thead>
<tr>
<th>Number</th>
<th>Control</th>
<th>Number</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Playbar</td>
<td>7</td>
<td>Playback speed selector</td>
</tr>
<tr>
<td>2</td>
<td>Scrub bar</td>
<td>8</td>
<td>Thumbnail</td>
</tr>
<tr>
<td>3</td>
<td>Scrub handle</td>
<td>9</td>
<td>Mute</td>
</tr>
<tr>
<td>4</td>
<td>Previous frame</td>
<td>10</td>
<td>Video quality selector</td>
</tr>
<tr>
<td>5</td>
<td>Play</td>
<td>11</td>
<td>Rotate</td>
</tr>
<tr>
<td>6</td>
<td>Next frame</td>
<td>12</td>
<td>Full screen</td>
</tr>
</tbody>
</table>
The following figure shows the media player controls that appear when the player is playing. Additionally, in the following figure, the sound is muted.

**Second Interview**

**Available Controls — Player Playing, Sound Muted**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Playbar</td>
</tr>
<tr>
<td>2</td>
<td>Scrub bar</td>
</tr>
<tr>
<td>3</td>
<td>Scrub handle</td>
</tr>
<tr>
<td>4</td>
<td>Previous event</td>
</tr>
<tr>
<td>5</td>
<td>Pause</td>
</tr>
<tr>
<td>6</td>
<td>Next event</td>
</tr>
<tr>
<td>7</td>
<td>Playback speed selector</td>
</tr>
<tr>
<td>8</td>
<td>Thumbnail</td>
</tr>
<tr>
<td>9</td>
<td>Mute</td>
</tr>
<tr>
<td>10</td>
<td>Video quality selector</td>
</tr>
<tr>
<td>11</td>
<td>Rotate</td>
</tr>
<tr>
<td>12</td>
<td>Full screen</td>
</tr>
</tbody>
</table>

**Long Video Playback Controls**

For all videos that are 10 minutes or more in length, additional controls and elements are available in the video navigation area. These controls allow users to more accurately set markers and create clips in long videos, along with providing finer controls for editing and redaction.
Information about the additional controls and elements is provided below.

### Long Video Playback Controls

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Time Slide Bar: Changes the section of the overall timeline that is shown. The size and position of the slide bar</td>
</tr>
<tr>
<td>2</td>
<td>Time marks: These provide additional guides for users, showing which part of video is being viewed and providing a time interval reference. As a user zooms in or out the timeline, the time values shown under the bar and intervals between marks change.</td>
</tr>
<tr>
<td>3</td>
<td>Blue Scrub Bar with vertical position line: Provides an indication of where you are in the video, as well as showing current buffer state in lighter blue. As video plays back the blue scrub bar grows and vertical line moves. When paused, this line acts as the placeholder for creating a new marker, clip, or redaction.</td>
</tr>
<tr>
<td>4</td>
<td>Hover line: When you position your mouse pointer over the navigation area, a grey vertical line appears showing a thumbnail with the video time. The thumbnail and time are updated as the pointer is moved. Clicking on navigation area jumps the blue scrub bar with vertical line to that point and updates main player. When the mouse pointer is not over navigation area, the hover line and thumbnail are no longer shown.</td>
</tr>
<tr>
<td>5</td>
<td>Zoom slider: Zooms in or out of the timeline. Zooming in allows users to be more precise when working with markers, clips, and editing tools.</td>
</tr>
</tbody>
</table>
Media Player Actions

The following table provides steps for the actions you can take with the media player.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Play</td>
<td>Click [play]</td>
</tr>
<tr>
<td>Play faster or slower</td>
<td>Click the playback speed selector until the speed you want is selected. You can choose from standard speed (1X), double speed (2X), or quadruple speed (4X).</td>
</tr>
<tr>
<td>View Thumbnails</td>
<td>Over the scrub bar, hover the mouse pointer above the time for which you want to see a thumbnail. A thumbnail image for the time appears.</td>
</tr>
<tr>
<td>Jump Ahead or Back</td>
<td>On the scrub bar, click and hold the scrub handle and drag it to the time in the media file that you want to go to.</td>
</tr>
<tr>
<td>Skip to Events</td>
<td>Click [prev] or [next] The video jumps to the previous or next marker or clip.</td>
</tr>
<tr>
<td>Pause</td>
<td>Click [pause]</td>
</tr>
<tr>
<td>View Frame by Frame</td>
<td>Click [prev] or [next].</td>
</tr>
<tr>
<td>View Full Screen</td>
<td>To enter full-screen viewing mode, click [full]. To exit full-screen viewing mode, click [exit].</td>
</tr>
<tr>
<td>Rotate Screen</td>
<td>1. Click [rotate].</td>
</tr>
<tr>
<td></td>
<td>2. Click [rotate].</td>
</tr>
<tr>
<td>Change video quality</td>
<td>1. Click [video quality].</td>
</tr>
<tr>
<td></td>
<td>2. Click the video quality that you want.</td>
</tr>
<tr>
<td>Mute, Unmute, or Control Volume</td>
<td>To mute audio, click [mute]. To unmute audio, click [unmute]. To raise or lower the audio volume, click and hold the audio slider and drag it left (quieter) or right (louder), as needed.</td>
</tr>
</tbody>
</table>

Multicam Playback

Note: Multicam playback will be added to all Axon Body 2, Axon Flex 2, and Fleet system cameras as part of the v1.9 camera firmware release, which began deployment in March 2017.

Multicam playback allows videos that were recorded by different cameras but in the same location and time to be viewed together. This allows users to view an incident from different vantage points at the same time. Up to four videos can be viewed at the same time.
Multicam Playback is only available for users with a Pro role and is not available for users with Lite or Basic roles.

During video recording, Axon Body 2, Axon Flex 2, and Fleet system cameras with v1.9 or later firmware will note when other Axon cameras are recording in the same vicinity, approximately 30 feet (10 meters), and add that information to the video file. When videos are uploaded to Evidence.com, that information is included in the upload so that the multicam playback option can be used.

When viewing evidence, the multicam action is shown as an option for any videos that are noted as having other videos that were recorded in the same vicinity at the same time.

Selecting Videos for Playback

When the user clicks Multicam on the evidence view, the multicam evidence selection page is shown and the user can select up to four related videos for simultaneous viewing. The upper section of the page shows the currently selected videos and the lower section has the list of related videos.

Note: Cameras must be within range of each other for at least one minute before or during recording, excluding pre-event buffering, for the videos to be displayed with multicam playback.
- Add a new video by clicking on a new tile in the upper section and then clicking the video name in the related video list.

- Change videos by clicking the tile in the upper section to select the video that will be replaced and then clicking the video name in the related video list.

- When all the videos have been selected, click **Launch Multicam**.

- Click **Back to Evidence** to return to the originally selected Evidence Detail page.

### Viewing Multiple Videos

When multicam playback is launched, the selected videos are requested from the system and synchronized. The upper section of page shows the videos and standard media player options, while the lower section shows information about the evidence files. The standard media player controls are also used for multicam playback.

During playback, videos that do not start at the beginning of the sequence show a message bar that states when the video will start. This allows users to easily know when a video will begin playing, so they can quickly jump to the point when all videos are active.
Since each video can have its own audio, an additional audio selector control was added to the media player controls. The audio selector is in the center of the media player controls and is used to select which audio track is used during playback.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicam Audio Control</td>
<td>To select the audio track for multicam playback, click ( \text{📖} ) and click on the video.</td>
</tr>
<tr>
<td></td>
<td>To view which audio track is being used, hover over ( \text{📖} ) and the ( \text{🎧} ) icon is shown.</td>
</tr>
<tr>
<td></td>
<td>Audio volume is still controlled by the audio slider.</td>
</tr>
</tbody>
</table>

**Requesting Transcriptions**

The on-demand transcription service allows you to order transcriptions of any video or audio stored in Evidence.com on a pay-as-you-go basis.

Transcriptions are normally completed within 24 hours of the request.

**Note:** Your User Role must have Order Transcript permission to use this functionality.

1. When viewing evidence, select the **Transcript** tab.

2. Click **Order Transcript**.

3. Enter additional information to add context which may help in accuracy of transcribing.

   Optionally, select to receive an email notification when the transcript is complete.
4. Click **Order Transcript**.

Once the transcript is complete, it is added to the Evidence Detail page and available for download.

### Transcript Status

After a transcript is ordered, the status of the order is shown in the Transcript tab.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order Submitted</td>
<td>The transcription order is being sent to the transcription service.</td>
</tr>
<tr>
<td>Order Received</td>
<td>The transcription order has been received by the transcription service, but has not been placed in a transcription queue.</td>
</tr>
<tr>
<td>Order Queued for Transcription</td>
<td>The transcription order is waiting to be processed.</td>
</tr>
<tr>
<td>Transcription in Progress</td>
<td>The transcription service is processing the transcription.</td>
</tr>
<tr>
<td>Order Complete</td>
<td>The transcription is complete, added to Evidence.com, and can be viewed from the Evidence page. If the email notification option was selected when ordering the transcript, an email notification is sent to the user,</td>
</tr>
<tr>
<td>Order On Hold</td>
<td>The transcription service has stopped work on the transcription. There can be a number of reasons for this, such as an agency budget limit was reached. Contact the transcription service for more information and resolution. Transcription service customer service contact information can be found on the Transcription Settings page. You might need to contact your Evidence.com administrator to get this information.</td>
</tr>
<tr>
<td>Canceled Order</td>
<td>The transcription order has been canceled. Note that orders can be reopened within 45 days of cancellation.</td>
</tr>
<tr>
<td>Failed to Send</td>
<td>This status is shown if a transcription order was sent more than 24 hours ago and the transcription service has not acknowledged the order. Contact your Evidence.com administrator to verify your agency's account with the transcription service is active and correctly set up.</td>
</tr>
<tr>
<td>Order Failed</td>
<td>The transcription service cannot complete the transcription. Contact the transcription service for more information and resolution. Transcription service customer service contact information can be found on the Transcription Settings page.</td>
</tr>
</tbody>
</table>
You might need to contact your Evidence.com administrator to get this information.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Creation Error</td>
<td>There was an issue with authenticating your account with the transcription service. Contact your Evidence.com administrator to verify your agency's account with the transcription service is active and correctly set up.</td>
</tr>
<tr>
<td>Order Reopened</td>
<td>The transcription service is reprocessing the transcription order.</td>
</tr>
</tbody>
</table>

**Sharing Transcripts**

When you share video or audio evidence, any associated transcripts requested by your agency are also shared with the selected users, agencies, or cases. However, if the recipient of the shared video or audio evidence orders a transcript, that transcript is not shared back to your agency. This ability will be available in a future release.

**Working with Markers and Clips**

Evidence.com provides markers and clips to help you work with video evidence.

- A *marker* is a pointer to a specific time in the evidence file. You can create a marker for any frame in an evidence file and assign a title and description to the marker.

  For video evidence, a marker is associated with single frame of a video evidence file. You can also download the marker as a picture file.

  For example, if a video includes a frame that shows an important detail, you can create a marker for that frame, which can be useful in several ways:

  - You can easily find important moments when you play the evidence file later.
  - Users with whom you share the evidence can easily locate moments that you have marked and read the title and description of the marker.
  - For video evidence only, you can download the marker as a picture file and send it to others in email or by other file sharing methods.

- A *clip* is a continuous segment of an evidence file that you can define. You can create a clip for any segment of an evidence file and assign the clip a title and description. For example, if a 10-minute video includes a 30-second segment that captures important actions and audio, you can create a clip for the important segment.
- You can easily play important segments of a media evidence file later.
- Users with whom you share the evidence can easily locate and play clips that you have created and read the title and description of the clip.
- When you want to share only a portion of an evidence file with others, you can extract a new media evidence file from the clip and share it rather than sharing the original evidence.
- You can redact a clip that you extract from a longer video evidence file, in order to reduce the amount of redaction work required.

**Marker and Clip Controls**

The controls for working with markers and clips appear below the scrub bar. The following figure the controls that appear when a media file has one marker and one clip.
### Marker and Clip Controls

<table>
<thead>
<tr>
<th>1 — Timeline</th>
<th>3 — Clip handles</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 — Marker handle</td>
<td>4 — Markers and clips list</td>
</tr>
</tbody>
</table>

### Add a Marker

You can create many markers in a media evidence file; however, you can only create one marker at a time.

1. On the Evidence Detail page, use the media player controls as needed until the scrub handle is at time that you want to mark.

   A common approach is to pause the player, click and hold the scrub handle, and then drag the scrub handle to the time that you want to mark.

2. Below the player, click **Clips & Markers**.

   The Add a Marker button appears below the Clips & Markers tab.

3. Click **Add Marker**.

   The new marker appears in the list of markers and clips.

   In the timeline below the player, the handle for the new marker appears at the frame currently shown in the player.

4. If you need to adjust the marker location, in the timeline, click and hold the marker handle, and then drag the marker handle to the time in the file that you want to mark.

5. If you want to change the title of the marker, in the list of markers and clips, click the marker, click ⌁ (edit), type the new title in the corresponding box, and then click **Save**.

   The marker you created is available in the list of markers and clips until you delete the marker.

### View a Marker

You can view a marker as needed, such as when you want to jump directly to an important moment while examining the contents of a media evidence file.

1. On the Evidence Detail page, below the player, click **Clips & Markers**.

   The list of markers and clips appears below the Clips & Markers tab.
2. In the list, click the marker that you want to view.

On the scrub bar, the scrub handle jumps to the frame that the marker points to.

**Edit a Marker**

You can make changes to an existing marker. For example, you may discover that a marker should point to a different frame. You may also need to change the title of an existing marker.

1. On the Evidence Detail page, below the player, click **Clips & Markers**.

The list of markers and clips appears below the Clips & Markers tab.

2. In the list, click the marker that you want to edit.

In the scrub bar, the scrub handle moves to the frame that the marker points to. On the timeline, the marker handle is highlighted.

3. If you need to adjust the marker location, in the timeline, click and hold the marker handle, and then drag the marker handle to the time in the file that you want to mark.

4. If you want to change the title of the marker, in the list of markers and clips, click the marker, click ✍️ (edit), type the new title in the corresponding box, and then click **Save**.

Evidence.com saves the changes you made to the marker.

**Download a Marker**

After you create a marker in video evidence file, you can download the frame that the marker points to as a JPG file. The file downloaded is named marker.jpg.

1. On the Evidence Detail page, below the player, click **Clips & Markers**.

The list of markers and clips appears below the Clips & Markers tab.

2. In the list, find the marker that you want to download.

At the right side of the marker is the Download button.

3. Click **Download**.

The download begins. The exact behavior depends on the browser you use and its download settings.
Add a Clip

You can create as many clips as you need. For example, if you want to share different segments of a media evidence file with different sets of users, you can create a clip for each set of users.

Each clip you create is independent of other clips for the same media evidence file. Clips can overlap. A shorter clip can be within a longer clip.

1. On the Evidence Detail page, below the player, click **Clips & Markers**.
   
   The Add a Clip button appears below the Clips & Markers tab.

2. Click **Add Clip**.
   
   The new clip appears in the list of markers and clips.

   In the timeline below the player, the start handle for the new clip appears in the timeline directly below the scrub handle. The end handle appears about one tenth of the file later. The content of the clip is the part of the timeline that is between the start and end handles.

3. On the timeline, select the segment of the file that you want in the clip.

   You can adjust the location of the start and end handles as needed until you have selected the exact portion of the video that you need in the clip.

   **| **Action** | **Steps** |
---|---|---|
| Move the start or end handle. | 1. On the timeline, hover the mouse pointer over the handle that you want to move.  
2. Press and hold the mouse button.  
3. Drag the handle left or right, as needed.  
4. Release the mouse button. |
| Move both handles together. | 1. On the timeline, hover the mouse pointer over the blue area between the start and end handles.  
2. Press and hold the mouse button.  
3. Drag the handles left or right, as needed.  
4. Release the mouse button. |

4. If you want to change the title of the clip, in the list of markers and clips, find the clip, click (edit), type the new title in the corresponding box, and then click **Save**.

   The clip you created is available in the list of markers and clips until you delete the clip.
Play a Clip

You can play a clip as needed. Especially for longer media files, you can save time by playing a clip that has been created to mark an important segment of a file.

If you intend to extract a new evidence file from a clip, you may want to play the clip to ensure it includes the content that you need.

1. On the Evidence Detail page, below the player, click **Clips & Markers**.
   
The list of markers and clips appears below the Clips & Markers tab.

2. In the list, click the clip that you want to view.
   
   On the scrub bar, the scrub handle jumps to the first frame of the clip.

3. On the playbar, click (play).
   
   Starting at the beginning of the clip, Evidence.com plays the file.

   For more information, see Media Player Actions.

Edit a Clip

You can make changes to an existing clip. For example, you may discover that a clip should have a different start or end. You may also need to change the title or description of an existing clip.

1. On the Evidence Detail page, below the player, click **Clips & Markers**.
   
The list of markers and clips appears below the Clips & Markers tab.

2. In the list, click the clip that you want to edit.
   
   In the scrub bar, the scrub handle moves to the start frame of the clip. On the timeline, the segment between the start and end handle of the clip is highlighted.

3. If you want to change start or end of the clip, on the timeline, adjust the location of the start and end handles until you have selected the exact portion of the file that you need in the clip.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
</table>
   | Move the start or end handle. | 1. On the timeline, hover the mouse pointer over the handle that you want to move.  
<p>|                          | 2. Press and hold the mouse button.                                     |
|                          | 3. Drag the handle left or right, as needed.                            |
|                          | 4. Release the mouse button.                                            |</p>
<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move both handles together.</td>
<td>1. On the timeline, hover the mouse pointer over the blue area between the start and end handles.</td>
</tr>
<tr>
<td></td>
<td>2. Press and hold the mouse button.</td>
</tr>
<tr>
<td></td>
<td>3. Drag the handles left or right, as needed.</td>
</tr>
<tr>
<td></td>
<td>4. Release the mouse button.</td>
</tr>
</tbody>
</table>

4. If you want to change the title of the clip, in the list of markers and clips, find the clip, click (edit), type the new title in the corresponding box, and then click **Save**.

Evidence.com saves the changes you made to the clip.

### Extract a New File from a Clip

After you create a clip, you can use it to extract a new evidence file at any time. Extracting a file from a clip creates a new evidence file whose start and end are exactly those that you specified in the clip. Evidence files created by extracting a clip appear in evidence searches. The file from which a clip is extracted is known as the **parent file**.

You can extract a file from a clip more than once. Each time you extract a file, a new evidence file is created. If the title of the clip is the same each time you extract a file from the clip, the files created have identical titles.

A file extracted from a clip inherits the metadata of the parent file, such as the case IDs, categories, tags, and evidence location. Inheriting the metadata helps ensure that extracted files are associated with the correct cases and that the applicable evidence retention policy is enforced, including any restricted categories. In addition, Evidence.com applies the tag “AXONclip” to the extracted file.

On the Evidence Detail page for evidence created by extracting a file from a clip, Evidence.com displays the title of the parent files and provides a link to the parent file.

1. On the Evidence Detail page, below the player, click **Clips & Markers**.
   
   The list of markers and clips appears below the Clips & Markers tab.

2. In the list, find the clip that you want to extract.

   At the right side of the clip is the Extract button.

3. Click **Extract**.
4. On the notification message box, click **Okay**.

Below the redaction, an extraction object appears, with a status of “Processing”.

Evidence.com begins extracting the clip as a new evidence file. When the extraction is complete, Evidence.com sends you a notification email.

### Delete a Marker or Clip

If you no longer need a marker or clip, you can delete it. You cannot restore a deleted marker or clip.

1. On the Evidence Detail page, below the player, click **Clips & Markers**.

   The list of markers and clips appears below the Clips & Markers tab.

2. In the list, find the marker or clip that you want to delete.

   At the right side of the marker or clip is the **(delete)** button.

3. Click **(delete)** and then click **Delete**.

   Evidence.com deletes the marker or clip. It no longer appears in the list of markers and clips.

### Video Evidence Redaction

Evidence.com provides the ability to redact what can be seen and heard in video evidence files. The redaction tools enable you to create redacted versions of video evidence files without affecting the original file.

**Note:** If you are looking for information on using the Redaction Studio feature, see the [Redaction Studio section](#) of this guide.

In Evidence.com, a *redaction* is a set of information that tells Evidence.com what to redact in a video. You can create a redaction with any of the Evidence.com redaction tools:

- Manual redaction
- Assisted redaction, also known as Smart Tracker redaction
• Skin Blur redaction

You can create and maintain many redactions for each video evidence file. This enables you to create different redacted videos for different audiences or different purposes.

When you have completed creating or editing a redaction manually or with Smart Tracker, you can extract a redacted video.

An extracted video is a video evidence file that Evidence.com creates from a clip or a redaction. Evidence.com never alters the original video evidence file when you create a clip or a redaction.

The clips and redactions features complement each other. If you have a long video and need to share a redacted segment, it is recommended that you first create a clip, extract a video from the clip, and then redact the extracted video.

**Note:** Skin Blur redaction cannot be done on clips.

---

**Manual Redaction**

Manual redaction allows you to create and control the size, shape, and placement of redaction masks precisely, frame by frame. You can also create and configure audio masks in order to mute the sound of specific video evidence-file segments.

For videos that are longer than about five minutes, it is recommended that you use assisted redaction.

**Manual Redaction Workflow**

When you use manual redaction, the process for creating a redacted video evidence file involves the procedures identified in the following steps.

1. Follow the steps in [Create a Redaction Manually](#).

2. Use the redaction to make a new, redacted video evidence file. Follow the steps in [Extract a Redacted Video from a Redaction](#).

3. Wait for Evidence.com to notify you by email that the extracted video is available.

4. Review the extracted video *carefully*, to ensure that it is redacted correctly. You can access the extracted video from a link provided in the notification email. For additional information, see [View Videos Extracted from Clips, Markers, and Redactions](#).

5. If you found redaction issues in the extracted video, edit the redaction as needed in order to correct the issues, and then return to step 2.

To edit the redaction, follow the steps in [Edit a Redaction](#).
6. If the extracted video is correctly redacted, use the extracted video as needed. For example, you can share it with others or download it, as you would any other video evidence file.

**Manual Redaction Concepts**

Creating a redaction manually involves working with several important concepts.

- **Object**—Organizes mask segments that redact the same actual object. A redaction contains one or more objects. Manual redaction supports two types of objects:
  - **Video object**—Organizes mask segments that redact one visual object. A video object contains one or more mask timelines.
  - **Mute object**—Organizes mask segments that redact portions of the sound in the video evidence file. The Mute object contains one mask timeline.

- **Mask**—Defines a rectangular area in a continuous segment of video frames that are redacted. Masks in a video object have three dimensions:
  - Height, defined by the mask frame.
  - Width, defined by the mask frame.
  - Duration, defined by the start and end handles of the mask segment.

  Manual redactions allow small height and width, for better redaction of small objects.

  Masks in the Mute object have only duration and therefore have a mask segment only and do not have a mask frame.

- **Mask timeline**—Represents all frames in the video and enables you to place the mask segment precisely where you need it. Each mask timeline has one mask segment.

- **Mask segment**—Defines the continuous series of frames that the mask redacts. A mask segment has a start and an end handle.

- **Mask segment handle**—Defines the start or end frames of a mask segment.

- **Mask frame**—Defines the rectangular area redacted by a mask in a video object. Masks in the Mute object do not have mask frames.

- **Mask frame handle**—Enables you to change the size and shape of the mask frame.
- **Blur level selector**—Enables you to specify how blurry the area inside a mask should appear in a video file extracted from a redaction. The selector supports four levels of blur:

<table>
<thead>
<tr>
<th>Light blur</th>
<th>Heavy blur</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium blur</td>
<td>Blackout</td>
</tr>
</tbody>
</table>
Manual Redaction Controls

1 — Mask frame
2 — Mask frame handle
3 — Blur level selector
4 — Video object
5 — Mute object
6 — Mask timeline
7 — Mask segment
8 — Mask segment handles
9 — Start and end times for the currently selected mask segment
**Smart Tracker Assisted Redaction**

Smart Tracker assisted redaction brings intelligent, automated support to your agency's video redaction workload. Using assisted redaction, you can easily create a redaction that tracks up to 10 objects in a video. For each object, you specify a start and end frame. On each start frame, you place and size a redaction mask.

When you are done preparing an assisted redaction, Smart Tracker tracks the masked objects automatically and Evidence.com sends you a notification email when it has finished creating the redaction.

It is recommended that you closely verify redactions created by assisted redaction. If you need to make corrections, Evidence.com enables you to edit the redaction manually.

**Smart Tracker Assisted Redaction Workflow**

When you use assisted redaction, the process for creating a redacted video evidence file involves the procedures identified in the following steps.

1. Follow the steps in Create a Redaction with Assisted Redaction.

2. Wait for Evidence.com to notify you by email that Smart Tracker has finished creating the redaction.

3. Review the redaction and edit it as necessary.

   You can access the video evidence file from a link provided in the notification email.

   You may need to edit the redaction for various reasons:

   - To correct the duration placement of masks
   - To change the blur level of masks
   - To add the Mute object and place mask segments as needed in order to redact audio.

   To edit the redaction, follow the steps in Edit a Redaction.

   **Note:** You may find it easier to skip step 3 and focus on reviewing the extracted video in step 6.

4. Use the redaction to make a new, redacted video evidence file. Follow the steps in Extract a Redacted Video from a Redaction.

5. Wait for Evidence.com to notify you by email that the extracted video is available.
6. Review the extracted video carefully, to ensure that it is redacted correctly. You can access the extracted video from a link provided in the notification email. For additional information, see View Videos Extracted from Clips, Markers, and Redactions.

7. If you found redaction issues in the extracted video, edit the redaction as needed in order to correct the issues, and then return to step 3.

To edit the redaction, follow the steps in Edit a Redaction.

8. If the extracted video is correctly redacted, use the extracted video as needed. For example, you can share it with others or download it, as you would any other video evidence file.

### Smart Tracker Assisted Redaction Concepts

Using assisted redaction and Smart Tracker technology to create a redaction shares many concepts with manual redaction. The following information explains assisted redaction concepts that differ those described in Manual Redaction Concepts.

Because Smart Tracker technology automatically tracks objects in the video file, the assisted redaction feature represents an object and its timeline with one control, eliminating the need for you to create multiple mask timelines per object.

- **Object**—Enables you to redact one actual object in the video. An assisted redaction object contains only one object timeline. Assisted redaction supports up to 10 objects.

  Assisted redaction supports redaction of video objects only. If you need to redact any portion of the audio track of a video evidence file, you can do so by editing the redaction that assisted redaction creates for you.

- **Object timeline**—Represents all frames in the video and enables you to place the mask segment precisely where you need it. Each object timeline has one mask segment.
### Smart Tracker Assisted Redaction Controls

1. Mask frame
2. Mask frame handle
3. Object and object timeline
4. Mask segment
5. Mask segment handles
6. Start and end times for the currently selected mask segment
Redaction Workflow Comparison

The following figure shows the process for redacting a video manually and for using Smart Tracker assisted redaction.

Begin with manual redaction

Create a redaction manually

Begin with Smart Tracker

Create a redaction with assisted redaction

Smart Tracker creates the redaction

Review redaction

Redact audio, set blur level, or make other adjustments?

Yes

Edit redaction

No

Adjustments needed?

Yes

Use redacted video as needed

Evidence.com finishes extracting video

Review redacted video

Extract new redacted video

No
Create a Redaction Manually

Administrators and users who are allowed the Redact permission can use the manual redaction tool to create a redaction for a video evidence file that is in a file format supported by the media player.

1. On the Evidence Detail page, below the video player, click Redactions.

   The Create New Redactions button appears below the Redactions tab. If any redactions already exist, they are listed below the buttons.

2. Click Create New Redactions.

   The Create a New Redaction dialog is shown.


   The controls for editing a manual redaction appear below the media player. Evidence.com creates the first object for you. Within the object is one mask.

4. For each additional object that you want to redact, click New Redaction. For example, if you need to redact three faces, you can add two more objects.

   Each new object appears at the bottom of the list of objects. Each new object contains one mask segment.

   If you need to delete an object, at the right end of the object, click Delete.

5. If you want to redact any portion of the audio track, click Audio Mute.

   The Mute object appears below the video objects. The Mute object contains one mask segment.

6. For each video object or the Mute object, create and configure mask segments, and for video objects, place the mask within each segment.

   Use as many mask segments as needed in order to redact the object. The following table lists the actions for configuring mask segments and masks.

<table>
<thead>
<tr>
<th>Action</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a mask segment to an object</td>
<td>At the right end of the object, click Add Mask.</td>
</tr>
</tbody>
</table>
| Delete a mask segment from an object | 1. If the mask segment is not blue, click the mask segment. Blue indicates that the mask segment is selected.  
  2. Click Delete Selection. |
<table>
<thead>
<tr>
<th>Action</th>
<th>Method</th>
</tr>
</thead>
</table>
| Move a start or end mask segment handle | To place a mask handle approximately at the frame you need:  
1. On the mask timeline, hover the mouse pointer over the mask segment handle that you want to move.  
2. Press and hold the mouse button.  
3. Drag the handle left or right, as needed.  
4. Release the mouse button.  
To move a mask handle one frame at a time:  
5. If the mask segment is not blue, click the mask segment. Blue indicates that the mask segment is selected.  
6. Use the keyboard controls, as needed:  
   - The “a” key — Move the start handle to the left, one frame at a time.  
   - The “s” key — Move the start handle to the right, one frame at a time.  
   - Left Arrow key — Move the end handle to the left, one frame at a time.  
   - Right Arrow key — Move the end handle to the right, one frame at a time. |
| Move both mask segment handles together | 1. On the mask timeline, if the area between the mask segment handles is not blue, click between the handles.  
2. Hover the mouse pointer over the blue area between the start and end handles.  
3. Press and hold the mouse button.  
4. Drag the handles left or right, as needed.  
5. Release the mouse button. |
| Move mask segment handles to specific times | 1. If the mask segment is not blue, click the mask segment. Blue indicates that the mask segment is selected.  
2. In the **Start** box, enter the exact time in minutes and seconds, in *mm:ss* format, where you want the start handle.  
3. In the **End** box, enter the exact time in minutes and seconds, in *mm:ss* format, where you want the end handle. |
| Move a mask frame in a mask segment | 1. If the mask segment is not blue, click the mask segment in order to ensure that you are moving the correct mask frame. In the player, the frame for the selected segment is red.  
2. In the media player, click the mask frame in order to select it.  
3. Click and hold the frame, avoiding the handle at the lower-right corner of the frame.  
4. Drag the frame to where you want it.  
5. Release the mouse button. |
| Shape a mask frame | 1. Click the mask segment in order to ensure that you are shaping the correct mask frame. In the player, the frame for the selected segment is red.  
2. At the lower-right corner of the frame, click and hold the handle.  
3. Drag the corner to where you want it.  
4. Release the mouse button. |
### Change the blur level of a mask

| Action                              | Method                                                                 | 1. Click the mask segment in order to ensure that you are setting the blur level for the correct mask. In the player, the frame for the selected segment is blue. | 2. Click the blur selector until the blur level you want is selected. You can select Light, Normal, Heavy, or Blackout. |

7. When you have finished configuring the redaction, click **Done**.

The Redactions tab reappears. The new manual redaction appears in the list of redactions. The redaction you created is available in the list of redactions until you delete the redactions.

### Edit a Redaction

You can edit the objects, mask segments, and mask frames of a redaction created manually or created with assisted redaction. Editing a redaction is the same process for both of these redaction types.

1. On the Evidence Detail page, below the video player, click **Redactions**.

   Existing redactions are listed below the Redactions tab.

2. In the list, find the redaction that you want to edit and then click **edit**.

   The controls for editing a manual redaction appear below the media player, including any objects and mask segments that the redaction contains.

3. If you need to add or remove objects, use methods provided in the following table.

<table>
<thead>
<tr>
<th>Action</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a video object</td>
<td>Click <strong>New Redaction</strong>. A new object appears in the list of objects. Each new object contains one mask segment.</td>
</tr>
<tr>
<td>Add the Mute object</td>
<td>Click <strong>Audio Mute</strong>. The Mute object appears below the video objects.</td>
</tr>
<tr>
<td>Delete an object</td>
<td>At the right end of the object that you want to add a mask segment to, click <strong>Delete</strong>. The object and any mask segments it contained are removed from the redaction.</td>
</tr>
</tbody>
</table>
4. If you need to edit mask segments or masks, use the methods provided in the following table.

<table>
<thead>
<tr>
<th>Action</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a mask segment to an object</td>
<td>At the right end of the object, click <strong>Add Mask</strong>.</td>
</tr>
</tbody>
</table>
| Delete mask segment from an object | 1. If the mask segment is not blue, click the mask segment. Blue indicates that the mask segment is selected.  
2. Click **Delete Selection**. |
| Move the start or end mask segment handle | To place a mask handle approximately at the frame you need:  
1. On the mask timeline, hover the mouse pointer over the mask segment handle that you want to move.  
2. Press and hold the mouse button.  
3. Drag the handle left or right, as needed.  
4. Release the mouse button.  
To place a mask handle precisely at the frame you need:  
1. If the mask segment is not blue, click the mask segment. Blue indicates that the mask segment is selected.  
2. Use the keyboard controls, as needed:  
   1. The “a” key — Move the start handle to the left, one frame at a time.  
   2. The “s” key — Move the start handle to the right, one frame at a time.  
   3. Left Arrow key — Move the end handle to the left, one frame at a time.  
   4. Right Arrow key — Move the end handle to the right, one frame at a time. |
| Move both mask segment handles together | 1. On the mask timeline, if the area between the mask segment handles is not blue, click between the handles.  
2. Hover the mouse pointer over the blue area between the start and end handles.  
3. Press and hold the mouse button.  
4. Drag the handles left or right, as needed.  
5. Release the mouse button. |
| Move mask segment handles to specific times | 1. If the mask segment is not blue, click the mask segment. Blue indicates that the mask segment is selected.  
2. In the **Start** box, enter the exact time in minutes and seconds, in *mm:ss* format, where you want the start handle.  
3. In the **End** box, enter the exact time in minutes and seconds, in *mm:ss* format, where you want the end handle. |
<table>
<thead>
<tr>
<th>Action</th>
<th>Method</th>
</tr>
</thead>
</table>
| Move a mask frame in a mask segment       | 1. If the mask segment is not blue, click the mask segment in order to ensure that you are moving the correct mask frame. In the player, the mask frame for the selected segment is red.  
2. In the media player, click the mask frame in order to select it.  
3. Click and hold the frame, avoiding the handle at the lower-right corner of the frame.  
4. Drag the frame to where you want it.  
5. Release the mouse button. |
| Shape a mask frame                         | 1. Click the mask segment in order to ensure that you are shaping the correct mask frame. In the player, the mask frame for the selected segment is red.  
2. At the lower-right corner of the frame, click and hold the handle.  
3. Drag the corner to where you want it.  
4. Release the mouse button. |
| Change the blur level of a mask            | 1. Click the mask segment in order to ensure that you are setting the blur level for the correct mask. In the player, the frame for the selected segment is blue.  
2. Click the blur selector until the blur level you want is selected. You can select Light, Normal, Heavy, or Blackout. |

5. When you have finished editing the redaction objects, mask segments, and mask frames, do one of the following actions:

- If you want to save all your edits to the redaction, click **Done**. Evidence.com saves the changes to the redaction.

- If you do not want to save any edits to the redaction, click **Cancel**. Evidence.com discards any changes made to the redaction.

The Redactions tab reappears.

**Create a Redaction with Smart Tracker Assisted Redaction**

Administrators and users who are allowed the Redact permission can use Smart Tracker assisted redaction to create a redaction for a video evidence file that is in a file format supported by the media player.

Smart Tracker assisted redaction supports redaction of video objects only. If you need to redact any portion of the audio track of a video evidence file, you can do so by editing the redaction that assisted redaction creates for you.

1. On the Evidence Detail page, below the video player, click **Redactions**.
The Create New Redactions button appears below the Redactions tab. If any redactions already exist, they are listed below the buttons.

2. Click **Create New Redactions**.

The Create a New Redaction dialog is shown.

3. Select **Smart Tracker** and click **Start**.

The assisted redaction controls replace the media player. Evidence.com creates the first object timeline for you. The timeline has one mask segment.

4. For each additional object that you want to redact, click **New Redaction**. For example, if you need to redact three faces, you can add two more objects.

Each new object timeline appears at the bottom of the list of objects. Each new object contains one mask segment.

If you need to delete an object, click the object in order to ensure that it is selected, and then click **Delete Selection**.

5. For each object, set the start and end frame, and then place and size the mask frame.

For best results, it is recommended that you size mask frames so that they are 20 to 30% larger than the actual object that you want to redact.

<table>
<thead>
<tr>
<th>Action</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move the start or end mask segment handle</td>
<td>To place a mask handle approximately at the frame you need:</td>
</tr>
<tr>
<td></td>
<td>1. On the mask timeline, hover the mouse pointer over the mask segment handle that you want to move.</td>
</tr>
<tr>
<td></td>
<td>2. Press and hold the mouse button.</td>
</tr>
<tr>
<td></td>
<td>3. Drag the handle left or right, as needed.</td>
</tr>
<tr>
<td></td>
<td>4. Release the mouse button.</td>
</tr>
<tr>
<td></td>
<td>To place a mask handle precisely at the frame you need:</td>
</tr>
<tr>
<td></td>
<td>1. If the mask segment is not blue, click the mask segment. Blue indicates that the mask segment is selected.</td>
</tr>
<tr>
<td></td>
<td>2. Use the keyboard controls, as needed:</td>
</tr>
<tr>
<td></td>
<td>o The “a” key — Move the start handle to the left, one frame at a time.</td>
</tr>
<tr>
<td></td>
<td>o The “s” key — Move the start handle to the right, one frame at a time.</td>
</tr>
<tr>
<td></td>
<td>o Left Arrow key — Move the end handle to the left, one frame at a time.</td>
</tr>
<tr>
<td></td>
<td>o Right Arrow key — Move the end handle to the right, one frame at a time.</td>
</tr>
<tr>
<td>Action</td>
<td>Method</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Move both mask segment handles together</td>
<td>1. On the object timeline, if the area between the mask-segment handles is not blue, click between the handles.</td>
</tr>
<tr>
<td></td>
<td>2. Hover the mouse pointer over the blue area between the start and end handles.</td>
</tr>
<tr>
<td></td>
<td>3. Press and hold the mouse button.</td>
</tr>
<tr>
<td></td>
<td>4. Drag the handles left or right, as needed.</td>
</tr>
<tr>
<td></td>
<td>5. Release the mouse button.</td>
</tr>
<tr>
<td>Move mask segment handles to specific times</td>
<td>1. If the mask segment is not blue, click the mask segment. Blue indicates that the mask segment is selected.</td>
</tr>
<tr>
<td></td>
<td>2. In the <strong>Start</strong> box, enter the exact time in minutes and seconds, in <em>mm:ss</em> format, where you want the start handle.</td>
</tr>
<tr>
<td></td>
<td>3. In the <strong>End</strong> box, enter the exact time in minutes and seconds, in <em>mm:ss</em> format, where you want the end handle.</td>
</tr>
<tr>
<td>Move the mask frame in a mask segment</td>
<td>1. If the mask segment is not blue, click the mask segment in order to ensure that you are moving the correct mask frame.</td>
</tr>
<tr>
<td></td>
<td>In the player, the mask frame is red.</td>
</tr>
<tr>
<td></td>
<td>2. In the start frame, click and hold the mask frame, avoiding the handle at the lower-right corner of the frame.</td>
</tr>
<tr>
<td></td>
<td>3. Drag the frame to where you want it.</td>
</tr>
<tr>
<td></td>
<td>4. Release the mouse button.</td>
</tr>
<tr>
<td>Shape a mask frame</td>
<td>1. Click the mask segment in order to ensure that you are shaping the correct mask frame.</td>
</tr>
<tr>
<td></td>
<td>In the player, the mask frame is red.</td>
</tr>
<tr>
<td></td>
<td>2. At the lower-right corner of the frame, click and hold the handle.</td>
</tr>
<tr>
<td></td>
<td>3. Drag the corner to where you want it.</td>
</tr>
<tr>
<td></td>
<td>4. Release the mouse button.</td>
</tr>
</tbody>
</table>

6. When you have finished configuring assisted redaction, click **Done**.

The Redactions tab reappears. The new redaction appears in the list of redactions.

Smart Tracker begins processing the redaction.

When processing is complete, Evidence.com sends you a notification email.

**Extract a Redacted Video from a Redaction**

Extracting a video from a redaction is how you create a redacted video, which you can share or download as needed. After you create a redaction, you can extract a new video evidence file at any time. Extracting a redacted video from a redaction creates a new video evidence file that is redacted exactly how you specified when you created and edited the redaction. Video evidence created by extracting a redacted video appears in evidence searches. The video from which a redacted video was extracted is known as the *parent video*.
You can extract a redacted video from a redaction more than once. Each time you extract a redacted video, a new video file is created. If the title of the redaction is the same each time you extract a video from the redaction, the video files created have identical titles.

A video extracted from a redaction inherits the case IDs, categories, tags, and evidence location of the parent video. Inheriting this information helps ensure that extracted videos are associated with the correct cases and that the applicable evidence retention policy is enforced, including any restricted categories. In addition, Evidence.com applies the tag “AXONRedaction” to the video.

On the Evidence Detail page for a redacted video file, Evidence.com displays the title of the parent video file and provides a link to the parent video file.

1. On the Evidence Detail page, below the video player, click **Redactions**.

   The list of redactions appears below the Redactions tab.

2. In the list, find the redaction from which you want to extract a redacted video and then click **Extract**.

3. On the notification message box, click **Okay**.

   Evidence.com begins creating the new redacted video evidence file.

   Below the redaction, an extraction object appears, with a status of “Processing”.

   ![Extraction Object](image)

   When the extraction is complete, Evidence.com sends you a notification email.

### Delete a Redaction

You can delete redactions at any time; however, you cannot recover a deleted redaction. In order to prevent the work required to recreate a rashly deleted redaction, it is recommended that you ensure that a redaction is never needed again prior to deleting it.

Redacted videos extracted from a redaction are not affected when you delete the redaction from the parent video.

1. On the Evidence Detail page, below the player, click **Redactions**.

   The list of redactions appears below the Redactions tab.
2. In the list, find the redaction that you want to delete, click ⌘, and then click Delete.

Evidence.com deletes the redaction. It no longer appears in the list of redactions.

**Skin Blur Redaction**

With Skin Blur redaction, the user selects the level of skin blurring. Then, during processing, the redaction algorithm searches for skin tones throughout the video and blurs them to the selected level.

Skin blurring can only be used with the full-length video evidence file.

1. On the Evidence Detail page, below the video player, click Redactions.

   The Create New Redactions button appears below the Redactions tab. If any redactions already exist, they are listed below the buttons.

2. Click Create New Redactions.

   The Create a New Redaction dialog is shown.

3. Select Skin Blur and click Next.

4. Select the blur level you want to apply to the redaction and click Process.

5. The file is sent for redaction processing. Click Okay to acknowledge this action.

   The redaction is added to the evidence redaction list with a processing status.
When you receive notification that processing is complete, you can view the extracted redaction by clicking the email link or by going to the evidence, clicking the **Redactions** tab, and then clicking **View** for the file.

### Upload a Third-Party Redacted Video

Users can upload a video as a child of an existing evidence file. This enhancement embraces any current workflows of your agency with respect to video redaction, while still enabling your use of Evidence.com digital evidence management workflows.

Users can download the original piece of video evidence from the Evidence Detail page, redact that video with software outside of evidence.com, and then follow the steps below in order to upload the redacted video as a child of the original video evidence.

This feature helps you keep track of the redactions that you may have created outside of Evidence.com for specific video evidence. The uploaded redacted file inherits metadata from the original evidence. The parent-child relationship makes case organization, metadata management, and sharing easier. The uploaded redacted file appears under the Redactions tab clearly labeled as an uploaded redaction.

1. On the Evidence Detail page, below the player, click the **Redactions** tab.

   The Create New Redactions button appears below the Redactions tab. If any redactions already exist, they are listed below the buttons.

2. Click **Create New Redactions**.

   The Create a New Redaction dialog is shown.

3. Select **Redaction Upload** and click **Next**.

   The Upload Redaction dialog box appears.

4. Select the redacted video file that you want to import, using either of the following methods:

   - Find the file on your computer and then drag and drop the files onto the Upload Redaction dialog box.
   - Click **Choose Files** and then use the dialog box to find and select the file on your computer.

   By default, Evidence.com names the file “Redaction upload (original file name)”.

5. If you want to change the title of the file, click in the **Edit Title** box and change the title as needed.
6. Click **Upload**.

Evidence.com uploads the file. When the upload finishes, the uploaded file is listed on the Redactions tab.

---

**View Evidence Extracted from Clips, Markers, and Redactions**

Evidence.com keeps track of evidence files extracted from a parent file. This helps ensure that you are viewing the correct evidence file. It may also be more convenient if you aren't sure of the name given to an extracted file but do remember the name of the parent file.

1. Open the Evidence Detail page of the *parent* file.

2. Below the media player, click the **Redaction** tab or the **Clips & Markers** tab, as applicable.

   A list of redaction, clip, or marker objects appears, as applicable.

3. In the list, expand the object that the evidence was extracted from.

4. On the extraction that you want to view, click **View**.

   The Evidence Detail page of the extracted file opens.

5. Take the actions that you need. For more information, see Media Player Actions.

6. If you want to return to the Evidence Detail page of the parent file, next to **Parent file**, click the title.
Working with Image Evidence

Image evidence files are still images, such as scanned photographs, digital pictures, and screenshots. Evidence.com media tools include important features for working with image evidence files. The photo edit feature enables users to crop and rotate images, in addition to adjusting the brightness and contrast of images. From a photo edit, users can extract a new image evidence file that incorporates the edits, leaving the original image evidence file unaltered.

Photo Edit Controls

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cropping frame</td>
<td>Cropping frame handle</td>
<td>Rotate</td>
<td>Crop</td>
<td>Brightness slider</td>
<td>Brightness slider handle</td>
<td>Contrast slider</td>
<td>Contrast slider handle</td>
</tr>
</tbody>
</table>

Image Tool Controls

- 1 — Cropping frame
- 2 — Cropping frame handle
- 3 — Rotate
- 4 — Crop
- 5 — Brightness slider
- 6 — Brightness slider handle
- 7 — Contrast slider
- 8 — Contrast slider handle
**Photo Edit Workflow**

The following figure shows the process for creating a photo edit for an image evidence file and extracting a new, edited image.

```
Begin

Create a photo edit for an image

Extract a new edited image

Evidence.com extracts new edited image

Review extracted, edited image

Adjustments needed?

Yes

Edit the photo edit

No

Use extracted image as needed
```

**Create a Photo Edit**

Administrators and users who are allowed the Evidence Edit permission can use the photo edit tool to create an edited image from an image evidence file that is in a file format supported by the media player.

1. On the Evidence Detail page, below the video player, click *Edits*.

   The New Photo Edit button appears below the Edits tab. If any photo edits already exist, they are listed below the button.
2. Click (new photo edit).

The controls for configuring a photo edit appear below the image.

3. Use the controls to configure the photo edit.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rotate image</td>
<td>1. To rotate the image 90 degrees clockwise, click .</td>
</tr>
<tr>
<td></td>
<td>2. If you want to rotate the image more, continue clicking . until the image is rotated as needed.</td>
</tr>
<tr>
<td>Crop image</td>
<td>1. Click . The cropping frame appears over the image. The area inside the cropping frame is what appears in an image extracted from this photo edit.</td>
</tr>
<tr>
<td></td>
<td>2. On the image, click and hold the cropping frame, avoiding the handle at the lower-right corner of the frame.</td>
</tr>
<tr>
<td></td>
<td>3. Drag the frame to where you want it.</td>
</tr>
<tr>
<td></td>
<td>4. Release the mouse button.</td>
</tr>
<tr>
<td></td>
<td>5. At the lower-right corner of the frame, click and hold the cropping frame handle.</td>
</tr>
<tr>
<td></td>
<td>6. Drag the corner to where you want it.</td>
</tr>
<tr>
<td></td>
<td>7. Release the mouse button.</td>
</tr>
<tr>
<td></td>
<td>8. Until the frame position and shape are as needed, continue to move and shape the cropping frame.</td>
</tr>
<tr>
<td>Adjust brightness</td>
<td>1. On the brightness slider, click and hold the slider handle.</td>
</tr>
<tr>
<td></td>
<td>2. Drag the handle left or right, until the brightness is at the level that you need.</td>
</tr>
<tr>
<td></td>
<td>3. Release the mouse button.</td>
</tr>
<tr>
<td>Adjust contrast</td>
<td>1. On the contrast slider, click and hold the slider handle.</td>
</tr>
<tr>
<td></td>
<td>2. Drag the handle left or right, until the contrast is at the level that you need.</td>
</tr>
<tr>
<td></td>
<td>3. Release the mouse button.</td>
</tr>
</tbody>
</table>

4. When you have finished configuring the photo edit, click Done.

The Edits tab reappears. The new photo edit appears in the list of photo edits. Until you delete the photo edit that you created, it is available in the list of photo edits for the image.

Edit a Photo Edit

You can make changes to an existing photo edit. For example, you may discover that an extracted, edited image needs to be cropped differently.

1. On the Evidence Detail page, below the player, click Edits.

The list of photo edits appears below the Edits tab.
2. In the list, find the photo edit that you want to edit and then, at the right side of the photo edit, click 

The controls for configuring a photo edit appear below the image.

3. Use the controls to change the photo edit, as needed.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Rotate image                | 1. To rotate the image 90 degrees clockwise, click 
2. If you want to rotate the image more, continue clicking until the image is rotated as needed. |
| Remove image cropping      | Click . The cropping frame no longer appears on the image. \[Click .
Adjust image cropping       | If the cropping frame does not appear on the image, click .

To adjust the position of the cropping frame:
1. Click and hold the cropping frame, avoiding the handle at the lower-right corner of the frame.
2. Drag the frame to where you want it.
3. Release the mouse button.

To adjust the shape or size of the cropping frame:
1. At the lower-right corner of the frame, click and hold the cropping frame handle.
2. Drag the corner to where you want it.
3. Release the mouse button. |
| Adjust brightness          | 1. On the brightness slider, click and hold the slider handle. 2. Drag the handle left or right, until the brightness is at the level that you need. 3. Release the mouse button. |
| Adjust contrast            | 1. On the contrast slider, click and hold the slider handle. 2. Drag the handle left or right, until the contrast is at the level that you need. 3. Release the mouse button. |

4. Click Done.

Evidence.com saves the changes you made to the photo edit.
**Extract an Edited Image**

After you create a photo edit, you can extract an edited image from it at any time. Extracting an edited image creates a new image evidence file that is edited exactly how you specified when you created the photo edit. Image evidence created by extracting an edited image appears in evidence searches. You can share or download the extracted edited image as needed, without affecting or sharing the original image evidence.

You can extract an edited image from a photo edit more than once. Each time you extract an edited image, a new image file is created. If the title of the photo edit is the same each time you extract an image from the photo edit, the image files created have identical titles.

An image extracted from a photo edit inherits the case IDs, categories, tags, and evidence location of the original image. Inheriting this information helps ensure that extracted images are associated with the correct cases and that the applicable evidence retention policy is enforced, including any restricted categories.

On the Evidence Detail page for an extracted edited image, Evidence.com displays the title of the parent image file and provides a link to the parent image file.

1. On the Evidence Detail page, below the image, click **Edits**.
   
   The list of image edits appears below the Edits tab.

2. In the list, find the photo edit from which you want to extract an edited image and then click **Extract**.

3. On the notification message box, click **Okay**.
   
   Evidence.com begins creating the new edited image file.

   Below the redaction, an extraction object appears, with a status of “Processing”.

   ![Extraction Object](image)

   When the extraction is complete, Evidence.com sends you a notification email.
Evidence Map

In PRO agencies, administrators and users who are allowed the Evidence Search permission have access to the Evidence Map feature. The map shows icons for any evidence that has location information. For more information, see Edit Location.

The map icon used for an evidence file is determined by the evidence type. There are six icons that correspond to file types:

- Video
- Audio
- Document
- Image
- Firing Log
- Other

To view the evidence map, on the menu bar, click Evidence and then click Evidence Map.

In addition to searching for evidence using the map, you can use the same actions as on the other evidence search pages. See Working with Evidence Search Results for more information.

Basic Map Actions

The evidence map provides basic features for finding and viewing an evidence location on the map.
The following table describes the basic actions that are available on the evidence map.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pan</td>
<td>1. Position the mouse pointer over the map.</td>
</tr>
<tr>
<td></td>
<td>2. Click and hold the mouse button.</td>
</tr>
<tr>
<td></td>
<td>3. Move the mouse to pan the map.</td>
</tr>
<tr>
<td></td>
<td>4. Optionally, click <strong>Redo Search in this Area</strong> to see additional evidence in the new map view.</td>
</tr>
<tr>
<td>Zoom In or Zoom Out</td>
<td>• In the map, click on the + or − icons to zoom in or out.</td>
</tr>
<tr>
<td></td>
<td>Alternately, if your mouse has a mouse wheel:</td>
</tr>
<tr>
<td></td>
<td>1. Position the mouse pointer over the map.</td>
</tr>
<tr>
<td></td>
<td>2. Rotate the mouse wheel to zoom in or out.</td>
</tr>
<tr>
<td></td>
<td>If needed, click <strong>Redo Search in this Area</strong> to see additional evidence in the new map view.</td>
</tr>
</tbody>
</table>

When you click on a map icon, the map centers on that icon and shows a dialog box with information about the evidence. You can click View Evidence to go to the Evidence detail page or click anywhere on the map to close the dialog box.

**Searching from the Evidence Map**

1. To the left of the map, enter your search filter parameters.

   The Location filter is shown by default, click **Show Advanced Search** to see additional filters.
2. Specify the filters that you want to apply.

<table>
<thead>
<tr>
<th>Filter</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Location | 1. Click in the Location field.  
          | 2. Type in an address, city, or zip code.  
          | 3. Optionally, select |
| User     | 1. Click in the User field.  
          | 2. Start typing the name or badge ID of the user.  
          | 3. Wait for Evidence.com to show the matching users.  
          | 4. Click the user you want. |
| Date     | 1. Click in the Start or End field.  
          | 2. Select the date. |
| Category | Select the categories that you want to include on the evidence map. |

3. Click **Search**.

The evidence map shows only the evidence that matches the filters that you specified.
Redaction Studio

Redaction Studio provides the ability to redact what can be seen and heard in evidence files. The tools enable you to create redacted versions of evidence files without affecting the original file. You can create and maintain multiple redactions for an evidence file. This enables you to create different redacted videos for different audiences or different purposes.

Redaction Studio includes options for frame-by-frame manual redaction, Spray Paint redaction (manual redaction during playback), object-tracking redaction, and audio redaction. These options can be used separately or together.

With the new real-time object-tracking redaction, users can add object-tracker masks to a video and immediately playback the video to view the results of the tracker redaction, while the system is processing the results. If the objecttracker mask does not follow or cover the intended subject during playback, the user can stop the video and re-position the mask, which will reprocess the redaction from that point forward, enhancing the object-tracker mask accuracy. This allows the user to redact while simultaneously playing back the video.

Redaction Studio is supported on Internet Explorer 11 on Windows 8.1+ platforms, Microsoft Edge, Firefox, Chrome, and Safari browsers.

Redaction Studio Terms and Concepts

In Evidence.com, redaction is a term used to describe the blurring of objects and removal of audio from video evidence. The following terms describe the components in Redaction Studio used to create a redaction:

- **Video Mask** — A rectangular area on the video that defines the objects that are redacted in a continuous segment of video frames. Video masks have their height and width defined by a Mask Frame and their duration defined by a Mask Segment. There are two types of video masks, a Manual Mask and an Object Tracker mask.

- **Audio Mask** — A continuous segment on the Audio Track that defines the audio that is redacted. Audio masks have only duration, which is defined by a Mask Segment.

- **Mask Segment** — Defines the continuous series of frames that the audio or video mask redacts. A mask segment has a start and an end.

- **Segment Timeline** — The area below the audio track that shows all the video mask segments for the current redaction. This area allows users to easily find and select video masks.
• **Video Mask Frame** — Defines the rectangular area redacted by a mask in a video. Video mask frames can be manually moved and resized. After placement, Object Tracker video masks will automatically attempt to track the object they are placed over.

• **Video Mask Frame Handle** — Enables you to change the size and shape of the video mask frame.

• **Spray Paint Redaction** — A type of manual redaction where the user can click and hold on a manual mask during video playback at normal or half speed, and then use the mouse to follow the object the user wants to redact.

• **Blur selector** — Enables you to specify how blurred the area inside a video mask frame appears in the extracted video file. The selector supports four level of blur:

<table>
<thead>
<tr>
<th>Light blur</th>
<th>Heavy blur</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium blur</td>
<td>Blackout</td>
</tr>
</tbody>
</table>
Redaction Studio Layout and Controls

1. Extract button
2. Redaction Studio Save and Exit
3. Redaction Mask Type selectors
4. Video Mask Frame
5. Video Mask Frame Handle
6. Video playback and speed controls
7. Video Track
8. Audio Track
9. Segment Timeline
10. Start and end times for the selected mask
11. Blur Selector
12. Delete selected mask
13. Playback volume control mask
14. Video Mask segment for the selected mask
15. Audio Mask segment for the selected mask
16. Show help screen

Keyboard Controls

<table>
<thead>
<tr>
<th>Key</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spacebar</td>
<td>Play/Pause video</td>
</tr>
<tr>
<td>1</td>
<td>1x playback speed</td>
</tr>
<tr>
<td>2</td>
<td>2x playback speed</td>
</tr>
<tr>
<td>4</td>
<td>4x playback speed</td>
</tr>
<tr>
<td>D</td>
<td>Forward 1 frame at a time. Hold to play video at half speed.</td>
</tr>
<tr>
<td>E</td>
<td>Forward 2 seconds</td>
</tr>
<tr>
<td>A</td>
<td>Rewind 1 frame</td>
</tr>
<tr>
<td>Key</td>
<td>Action</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Q</td>
<td>Rewind 2 seconds</td>
</tr>
<tr>
<td>W</td>
<td>Increase selected video mask size</td>
</tr>
<tr>
<td>S</td>
<td>Decrease selected video mask size</td>
</tr>
<tr>
<td>M</td>
<td>Press and hold to place audio mask, release to set end of audio mask.</td>
</tr>
<tr>
<td>Del</td>
<td>Delete selected mask from the video frame</td>
</tr>
<tr>
<td>Arrow keys (up, down, left, right)</td>
<td>Move selected video mask</td>
</tr>
<tr>
<td>[ or ] (left or right bracket)</td>
<td>Trim mask segment start (left bracket) or end (right bracket) to the current playback time.</td>
</tr>
</tbody>
</table>

**Redaction Studio Best Practices**

The list below has some tips, tricks, and best practices for working with Redaction Studio.

- If you have a long video and only need to share a redacted portion, it is recommended that you first create a clip, extract a video from the clip, and then redact the extracted video.

- For redactions where there are multiple masks on a video, complete the redaction work for one mask before working with a different mask.

- Use the Start and End time field inputs to precisely set mask segment start and end times. This is especially useful when setting the length of audio masks.

- The selected blur level is applied to the complete mask segment. If you need to change the blur level for only a portion of a mask segment, you should add another mask.

- When redacting with a Manual Mask:
  - It is generally easier to reduce the end time for a mask segment than to keep extending it. When a manual mask is placed the mask segment length is approximately 3 seconds. After placing a mask, extend the length of the mask segment and then reduce the end time as you view the video.
  - Try using Spray Paint redaction for redactions where the object being redacted does not dramatically changes position.
  - You can split a manual mask segment by pressing the Del key. This basically deletes the manual mask from that video frame. This action can be used with Spray Paint redaction to create a larger gap between the new mask segments.
• When redacting with an Object Tracker mask:
  
  o It is generally easier to redact objects using larger masks.

  o If the mask is not tracking the object very well, go back to the beginning of the mask segment and resize the mask to tighten it around the object.

  o If the object being tracked leaves the video and mask remains on the video, slowly rewind the video to the point just before the object leaves the video and resize the mask.

  o When an object first enters a video, don't use an Object Tracker mask until at least 1/2 the object is visible. Use a Manual mask for redaction until 1/2 the object is visible.

**Using Redaction Studio**

1. On the Evidence Detail page for the evidence you want to redact, below the video player, click **Redactions**.

   The Redaction Studio and Redaction Tools buttons appear below the Redactions tab. If any redactions already exist, they are listed below the buttons.

2. Click **Redaction Studio**.

   This launches Redaction Studio within the browser window.

3. Select the type of redaction mask you want to place.
• **Manual Mask** – Click and drag on the video to place and size a mask. Manual masks are blue when selected.

You can manually reposition and resize the mask for each video frame using the Redaction Studio screen or keyboard controls.

Spray Paint redaction: After placing a manual mask, you can click and hold on the mask and then use the mouse to follow the object you want to redact during video playback at normal or half speed. This option can reduce the amount of time needed to create a manual redaction, but might not be useful in situations where the object dramatically changes position. When using this option, you must use the keyboard controls to increase (W key) or decrease (S key) the size of the mask.

• **Object Tracker** – Click and drag on the video to place and size the mask. Object Tracker masks are green when selected.

The system begins processing the object tracking from the mask and you can playback the video to observe the results. If, during playback, the object-tracker mask does not cover the intended subject, you can stop the video and reposition and resize the mask to enhance the object-tracker mask processing. The system processes the updated information each time the mask is repositioned or resized. This allows the user to always be working on the final project and improves the overall accuracy of the object-tracking processing.

• **Audio Mask** – Click in the Audio Track to place the mask. Audio masks are red when selected. If an audio mask is selected during playback, Redaction Studio will still play the audio for that mask. If an audio mask is not selected during playback, the audio is muted for masked portions of the audio track.

You can place an audio mask and change the duration of the mask segment using the Redaction Studio screen or keyboard controls.

You can add additional masks as needed to cover more objects in the video. You can use different mask types in the same redaction. We recommend that you have no more than 3 masks processing at the same time. Processing is shown by a series of dots in the mask and mask segment, as shown in the example image below.
4. Advance the video and adjust masks as needed. The following table lists the actions for configuring mask segments and masks.

<table>
<thead>
<tr>
<th>Action</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add another video mask</td>
<td>It is recommended that you stop video playback before placing new masks.</td>
</tr>
<tr>
<td></td>
<td>• Click on the type of redaction mask you want to use.</td>
</tr>
<tr>
<td></td>
<td>• Click and drag on the video to place and size the mask.</td>
</tr>
<tr>
<td>Add an audio mask:</td>
<td>It is recommended that you stop video playback before placing new masks.</td>
</tr>
<tr>
<td></td>
<td>• Click on the Audio redaction mask.</td>
</tr>
<tr>
<td></td>
<td>• Click on the Audio Track to place.</td>
</tr>
<tr>
<td>Delete a mask</td>
<td>• Click the mask you want to delete. The selected mask changes color, based on the redaction type (blue for manual, green for tracking).</td>
</tr>
<tr>
<td></td>
<td>• Click the delete icon.</td>
</tr>
<tr>
<td>Move a video mask</td>
<td>• Click the mask you want to move. The selected mask changes color, based on the redaction type (blue for manual, green for tracking).</td>
</tr>
<tr>
<td></td>
<td>• Use the arrow keys to move the mask OR</td>
</tr>
<tr>
<td></td>
<td>• Move the cursor over the mask until it turns into a four-arrow pointer.</td>
</tr>
<tr>
<td></td>
<td>• Click and hold to drag the mask to where you want it.</td>
</tr>
<tr>
<td></td>
<td>• Release the mouse button.</td>
</tr>
<tr>
<td>Change the size of a video mask</td>
<td>• Click the mask you want to resize. The selected mask changes color, based on the redaction type (blue for manual, green for tracking).</td>
</tr>
<tr>
<td></td>
<td>• Use the W (increase) or S (decrease) keys to change the size. OR</td>
</tr>
<tr>
<td></td>
<td>• Move the cursor over a corner of the mask until it turns into a double-headed-arrow pointer.</td>
</tr>
<tr>
<td></td>
<td>• Click and hold to drag the corner to resize the mask.</td>
</tr>
<tr>
<td></td>
<td>• Release the mouse button.</td>
</tr>
</tbody>
</table>

Continued on next page
<table>
<thead>
<tr>
<th>Action</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the blur level of a video mask</td>
<td>• Click the mask. The selected mask changes color, based on the redaction type (blue for manual, green for tracking).</td>
</tr>
<tr>
<td>segment</td>
<td>• Click the Blur Selector until the blur level you want is selected. You can select Light, Medium, Heavy, or Blackout.</td>
</tr>
<tr>
<td></td>
<td>Play faster or slower</td>
</tr>
<tr>
<td></td>
<td>• Click the playback speed selector until the speed you want is selected. You can choose from half speed (0.5), standard speed (1X),</td>
</tr>
<tr>
<td></td>
<td>double speed (2X), or quadruple speed (4X).</td>
</tr>
<tr>
<td>Adjust the start or end point for a mask</td>
<td>Note: The bracket keys ([ or ]) can be used to trim a mask segment to the current</td>
</tr>
<tr>
<td>segment.</td>
<td>• Click the mask. The selected mask changes color, based on the redaction type (blue for manual, green for tracking, red for audio).</td>
</tr>
<tr>
<td></td>
<td>• Move the cursor over the start or end of the mask segment on the audio or video track until it turns into a double-headed-arrow</td>
</tr>
<tr>
<td></td>
<td>pointer.</td>
</tr>
<tr>
<td></td>
<td>• Drag the segment left or right, as needed.</td>
</tr>
<tr>
<td></td>
<td>• Release the mouse button.</td>
</tr>
<tr>
<td>Adjust mask segment start or end point to a</td>
<td></td>
</tr>
<tr>
<td>specific time</td>
<td>• Click the mask. The selected mask changes color, based on the redaction type (blue for manual, green for tracking, red for audio).</td>
</tr>
<tr>
<td></td>
<td>• In the Start box, enter the exact time in minutes and seconds, in mm:ss format, where you want the mask segment to start.</td>
</tr>
<tr>
<td></td>
<td>• In the End box, enter the exact time in minutes and seconds, in mm:ss format, where you want the mask segment to end.</td>
</tr>
</tbody>
</table>

5. When you have finished adding and configuring all the masks, click **Extract**.

The redaction processing dialog box is displayed. Click **Okay** to continue.

Evidence.com begins processing the redaction. When processing is complete, Evidence.com sends you a notification email with a link to the redacted video.
6. Click X to exit Redaction Studio and return to the Evidence Detail page.

Note: All work done to a video in Redaction Studio is saved.
Case Management

Cases allow your agency to organize related evidence files, such as files that pertain to the same incident. Users can share cases with other users.

Case management features are available only in Evidence.com PRO agencies. In LITE agencies, the Case menu is unavailable.

Create Case

Administrators and users whose role is allowed the Create Case permission can create a case.

The Add Matching Evidence feature makes it easy to add evidence to a case while you are creating the case. The feature finds evidence files that have the same ID that you specify for the case.

1. On the menu bar, click Cases and then click Create Case.

The Create Case page appears.

2. Enter the case ID and double-check that it is correct.

3. Enter a useful description, and then click Submit.

Evidence.com searches for evidence files that have the same ID as the ID you specified for the case. The Add Matching Evidence page lists 40 evidence files at a time. By default, all evidence is selected.
4. On the Add Matching Evidence page, add as many of the evidence files to the case as you want. By default, all evidence is selected.

   - If you want to add evidence to the case, ensure that the check box to the left of the evidence is selected and then click **Add to Case**.

     If more than 40 evidence files match the case ID, you can add 40 at a time and click **Continue** to see the next set of files.

   - If you want to go to the case without adding some or any of the evidence found, click **Skip to Case**.

When you are finished adding evidence, Evidence.com displays the View Case page.

5. Use the case as needed. For more information about available actions, see Working with Cases.

### Case Search — All Cases, My Cases, and Shared Cases

Evidence.com provides case search features to help you find the cases that you need. In the Cases area, you can use any of the three case-search pages:

- **All Cases**—Finds all cases, including cases you may not have permission to view.

- **My Cases**—Finds cases that you own. The Owner filter is automatically set to your name.

- **Shared Cases**—Finds cases that have been shared with you by the case owner or another user with permission to share the case.
1. On the menu bar, click **Cases**.

The All Cases page lists all cases, sorted by the date they were last updated.

2. Search for the cases that you need. The following table provides steps for search-related tasks.

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>View a case</td>
<td>Click the ID of the case.</td>
</tr>
<tr>
<td>Find cases that you own</td>
<td>Click <strong>My Cases</strong>.</td>
</tr>
<tr>
<td>Find cases that are shared with you</td>
<td>Click <strong>Shared Cases</strong>.</td>
</tr>
</tbody>
</table>
| Change search results                     | 1. Update the case search filters. For more information, see Case Search Filters.  
                                          | 2. Click **Search**.                                                 |
| Sort search results                       | Click the column heading for **ID**, **Create Date**, or **Last Update Date**.  
                                          | To reverse the sort order, click the heading again.                  |
| Switch between page layout options (table or detailed) | On the **Page Layout** list, click the layout you want.               |

For information about the actions you can take from search results, see Working with Case Search Results.

**Case Search Filters**

Case search filters help you limit search results to the cases that you want to see. Evidence.com includes in search results only the cases that match *all* the search filters that you set.

- **ID** — Limits search results to cases whose ID includes the characters you enter in the ID box. For more information, see Text Search Details.

- **Category** — Limits search results to cases that are assigned to the category that you select. By default, search results include cases assigned to any category, including uncategorized cases.

- **Status** — Limits search results to cases whose status matches the status selected. By default, case searches include all statuses.

- **Owner** — Limits search results to cases owned by the user specified. To specify the user, click in the Owner box, start typing the name of the user, wait for Evidence.com to show the matching users, and then click the user you want.

On the My Cases page, the Owner filter is set to your name by default.
• **Tag** — Limits search results to cases whose tags includes the characters you enter in the Tag box. For more information, see Text Search Details.

• **Flagged** — Limits search results to cases whose flag status matches the flag status selected.

• **Date** — Limits search results by either the creation date of the case or the last date that the case was updated, as selected. You must also specify a date range by using the From and To boxes; otherwise, the search is not limited by date range. Search results are inclusive of the dates specified.
  - **From** — The start of the date range. If the From box is empty, the date range begins with the earliest possible date.
  - **To** — The end of the date range. If the To box is empty, the date range ends with today.

---

**Text Search Details**

The ID and Tag filters provide advanced text matching capability for case searches.

- You can enter letters, numbers, and the special characters: comma (,), dash (-), opening parentheses (()), closing parentheses ()), slash (/), and backslash (\).

- The text you enter can be a full or partial match of the data you are filtering. For example, if you enter 21 in the ID box, then any evidence with 21 in any portion of the ID is included in search results.

- You can search for more than one text string in a single filter by adding a space between the strings. This provides AND search functionality of the data you are filtering. For example, if you enter 12- 34 in the ID box, search results include any evidence with both 12- and 34 in the ID, such as 12-3456 and 12-7348.

- The order of text strings is irrelevant. For example, if you enter 78 21 in the ID box, search results include evidence with the ID 21378 and 17821.

- Capitalization for letter characters is irrelevant. For example, if you enter REDACT in the Tag box, search results include evidence with the Title REDACT, redact, and redaction.
Working with Case Search Results

On case search pages — All Cases, My Cases, or Shared Cases — you can take the actions described in this section.

View Case

You can view cases listed in case search results if any of the following are true:

- You own the case.
- The owner of the case has shared it with you.
- Your user role allows you to view all cases.
- You are an administrator.

1. Search for the case you want to view.
2. In the search results, click the ID of the case.

The View Case page opens.
For information about the actions you can take from the View Case page, see Working with Cases.

### Add a Category to Cases

You can add a category to one or more cases in search results.

1. Search for the cases that you want to add a category to.

2. For each case that you want to add a category to, select the check box to the left of the case.

3. Above the search results, click **Update Category**.

   A dialog box appears.

4. In the New Category list, click the category that you want to add to all selected cases and then click **Update**.

5. On the notification message box, click **OK**.

   The search results show the category that you assigned to the cases. If more than one category is assigned to cases, “Multiple” appears in the Category column for that case.

### Update the Status of Cases

You can change the status assigned to one or more cases in search results. If you want to change the status of a case to Deleted, see Delete Case.

1. Search for the cases whose status you want to update.

2. For each case whose status you want to update, select the check box to the left of the case.
3. Above the search results, click **Update Status**.
   A dialog box appears.

4. In the Status list, click the status that you want to assign to all selected cases and then click **Update**.

5. On the notification message box, click **OK**.
   The search results show the new status that you assigned to the cases.

**Delete Cases**

You can delete cases that are listed in case search results. Deleting a case changes the status of the case being Deleted.

**Note:** When you delete a case, Evidence.com removes all evidence from the case and Evidence.com begins enforcing the retention policy determined by the categories assigned to the evidence. This may result in evidence being immediately queued for deletion.

1. Search for the cases that you want to delete.

2. For each case that you want to delete, select the check box to the left of the case.

3. Above the search results, click **Delete**.
   A confirmation dialog box appears.

4. Click **OK**.

5. On the notification message box, click **OK**.

6. If you want to confirm that the case status is Deleted, click **Search**, locate the case in the search results, and view the case status.
**Reassign Cases**

When you need to change the owner of a case to another user or to a group, you can reassign the cases from the results of a case search.

If you reassign a case to a group, Evidence.com chooses one user from the group to be the case owner. Evidence.com assigns the other users to the case as members. When it chooses an owner, Evidence.com prioritizes the choice.

1. **Group monitor** — If the group has monitors, Evidence.com chooses the owner from the monitors of the groups, choosing at random if there is more than one monitor to choose from.

   Group member — If the group has no monitors, Evidence.com chooses the owner from among the members of the group, choosing at random if there is more than one member to choose from.

1. Search for the cases that you want to reassign to another user.

2. For each case that you want to reassign, select the check box to the left of the case.

3. Above the search results, click **Reassign**.

   A dialog box appears.

4. In the **Reassign To** box, start typing the name of the user or group to whom you want to assign the cases, wait for Evidence.com to show the list of matching users and groups, click the user or group that you want, and then click **Reassign**.

5. In the confirmation dialog box, click **OK**.

   The search results show that the user or group who you selected is now the case owner.

---

**Add a Member to Cases**

When you need to share a case with users who are in your agency, you can add users to cases from the results of a case search.

If you want to share a case with people in a partner agency, see Share a Case with a Partner Agency.

1. Search for the cases that you want to share.

2. For each case that you want to share, select the check box to the left of the case.
3. Above the search results, click **Add Member**.

A dialog box appears.

4. In the **Enter User** box, start typing the name of the user you want to share with, wait for Evidence.com to show the list of matching users, click the user that you want, and then click **Share**.

5. In the confirmation dialog box, click **OK**.

### Export Case Search Results

You can export the results of a case search in PDF, Microsoft Excel, text, or CSV format.

**Note:** When case search results are exported in Microsoft Excel or CSV format, the Device Assignee First Name and Last Name are split into separate columns and a Badge ID column is included.

If the search results contain more than 500 cases, Evidence.com exports the search results in 500-case segments and asks you to confirm the download of the next segment.

1. Search for cases and refine the search until the search results represent the case list that you want to export.

2. Above the search results, click **Export**.

3. In the **Select Format** list, click the file format that you want for the exported case search results and then, on the message box, click **Export**.

   The case search results download in the format that you specified.

   If the case search results contain more than 500 cases, only the first 500 cases are included in the downloaded file and Evidence.com displays a dialog box for downloading the next 500 cases in the search results.

4. If you want to export case search results for additional cases, click **OK** each time the dialog box appears.

   The case search results download in a separate file for each 500-case segment of the search results.

### Flag and Un-flag Cases

You can flag cases that you want to find more easily in the future. Case searches allow you to filter the search results by the flag status of cases.
On any case search page, each case in the search results has a Flag or Unflag button in the Actions column.
• Cases that are not flagged have a black 🆙 (flag) button.

• Cases that are flagged have a red 🆓 (unflag) button.

If you want to flag or un-flag a case, click 🆙 (flag) or 🆓 (unflag), as applicable.

Working with Cases

This section describes the actions available on the View Case page for any case.

Edit Case ID

On the View Case page, the case ID appears in the upper-left corner.

1. To the right of the case ID, click 🆙 (edit).

   The case ID becomes editable.

2. Change the case ID, as needed, and then click Save.

   The View Case page shows the updated ID.

Edit the Description of a Case

You can add or edit a description of the case.

On the View Case page, the description appears below the case.

1. To the left of Description, click 🆙 (edit).

   The description text becomes editable.

2. In the Description box, type a new description or edit the existing description.

3. Click Update.

   Evidence.com saves the case description changes.
Assign and Unassign Categories

On the View Case page, the Categories area appears below the case description. The Categories area lists the categories that the case is assigned to, if any.

1. To the right of **Categories**, click ![edit](edit).

   The “Select a category” list appears. If the case is already assigned to categories, a red X appears beside each assigned category.

   ![Categories](edit)

2. If you want to assign the case to a category, in the **Select a category** list, click the category and then click **Add**.

   The category appears at the bottom of the list of assigned categories.

3. If you want to remove the case from a category, click the red X next to the category and then, on the confirmation message box, click **OK**.

   Evidence.com removes the category from the list of assigned categories.

4. When you are finished editing category assignments, click **Done**.

Add and Remove Tags for Cases

Tags are labels that you can apply to cases and evidence. Adding tags to a case can help you find the case more easily later. Case searches allow you to filter the search results by tags.

Tags are labels that you can apply to cases. You can add tags to cases that you want to find more easily in the future. Case searches allow you to filter the search results by tags.

On the View Case page, the Tags area appears below the description and the Categories area. If any tags exist, they appear as tiles. The following figure shows an example of the Tags area that has one tag named, “McKinley”.

![Tags](McKinley)
### Action | Steps
--- | ---
Add tag | 1. Under **Tags**, click in the box.  
2. Start typing the tag. Evidence.com shows you a list of existing tags that start with the letters you typed.  
3. If the tag you want to apply appears in the list, click the tag.  
4. Otherwise, finish typing the tag and then press **Enter**. Evidence.com adds the tag to the case.

Remove tag | 1. Under Tags, find the tag that you want to remove.  
2. At the left end of tag, click **×**. Evidence.com removes the tag from the case.

---

**Notes and Cases**

You can post notes about a case. In addition to the text of the note, Evidence.com shows the author of the note and the date and time that the note was created and updated.

On the View Case page, the Notes area appears below the description, the Categories, and the Tags areas.

#### Add a Note

You can post a note to a case.

1. If necessary, scroll down and find the Notes area.

2. To the right of **Notes**, click **📝** (edit).

   An editable box appears in the Notes area.

3. In the box, type the note and then click **Add Note**.

   Under Notes, the new note appears, with your name and the creation date and time.

#### Edit a Note

You can edit notes that have previously been posted to a case.

1. If necessary, scroll down and find the Notes area.

2. To the right of the note, click **Edit**.

   The note text becomes editable.

3. Edit the note text as needed.
4. Click **Update**.

The changes to the note appear, with your name and the date and time that the edits occurred.

---

**Delete a Note**

You can delete notes that you have posted.

1. If necessary, scroll down and find the Notes area.

2. To the right of the note, click **Delete**.

3. On the confirmation dialog box, click **OK**.

The note no longer appears on the View Case page.

---

**Add Evidence to a Case**

From the View Case page, you can add evidence to the case you are viewing; however, you cannot add evidence to a case whose status is Deleted.

If a case is shared with partner agencies and you add evidence to the case, Evidence.com provides you the option of sharing the additional evidence with the partner agencies.

1. Above the Case Details area, click **Add Evidence**.

An evidence search page appears.

2. Search for the evidence that you want to add to the case.

   If you need to refine the search results, use the search filters as needed. For more information, see Evidence Search Filters.
3. For each evidence file that you want to add to the case, select the check box to the left of the evidence ID.

4. Click **Add to Case**.

5. On the confirmation message box, click **Yes**.

   A dialog box provides you the choice of continuing to add evidence or returning to the case.

   If the case is shared with partner agencies, the dialog box also includes the option to share the additional evidence with all the partner agencies with whom the case is shared.

   ![Confirmation dialog box](image)

6. If you want to continue adding evidence, click **Add More Evidence** and then return to step 2.

7. If you have finished adding evidence, do one of the following actions:
   
   - If the dialog box does not list partner agencies, click **Return to Case**.
   
   - If you want to share the additional evidence with the listed partner agencies, ensure that the **Share with listed partner check box** is selected, and then click **Update Partner and Return to Case**.
   
   - If you do not want to share the additional evidence with the listed partner agencies, clear the **Share with listed partner check box**, and then click **Return to Case**.

   The View Case page reappears.

   If you chose to share the additional evidence with partner agencies, Evidence.com notifies them that there is additional evidence.

8. If you want to confirm that the evidence was added to the case, click **All Evidence** and view the list of evidence files assigned to the case.
Remove Evidence from a Case

From the View Case page, you can remove evidence from the case you are viewing.

Note: If the case and the evidence you are removing is shared with partner agencies, removing the evidence from the case in your agency has no effect on the copy of the case in partner agencies.

1. On the View Case page, click an evidence folder that the evidence is in.

   Below the evidence preview area, a list of evidence in the case appears.

2. For each evidence file that you want to remove from the case, select the check box to the left of the evidence file.

3. Above the evidence list, click Remove from Case.

4. On the confirmation dialog box, click Remove.

5. On the notification message box, click OK.

   Evidence.com removes the evidence from the case. The evidence list updates to reflect the removal of the evidence.

Work with Evidence Folders

Evidence folders provide you a way to organize evidence files. After you add evidence to a case, you can add the evidence to as many folders as you need. For example, you could create a folder for all evidence files in the case that prove a particular fact.

The All Evidence folder always includes all evidence in a case. You cannot delete the All Evidence folder.

You can add as many folders as you need; however, after you add folder, you cannot rename it. Instead of renaming a folder, you can create a new folder, add the evidence from the old folder to the new folder, and then remove the old folder.

Add a Folder

1. On the View Case page, below the case ID, click Add Folder.

2. On the dialog box, in the Enter Folder Name box, type a meaningful name for the folder, and then click Add.

   Evidence.com creates the folder and adds it to the list of folders below the case ID.
**Delete a Folder**

You can delete any folder that you created. You cannot delete the All Evidence folder.

1. On the View Case page, below the case ID, click **Delete Folder**.

2. On the dialog box, in the **Select Folder** list, click the folder that you want to remove, and then click **Delete**.

3. On the notification message box, click **OK**.

**Add Evidence to a Folder**

For evidence that is already in a case, you can add the evidence to any evidence folder that you need.

If you need to add evidence to the case, see Add Evidence to a Case.

1. On the View Case page, click an evidence folder that the evidence is already in.

   **Note:** You can always use the All Evidence folder for this purpose.

   Below the evidence preview area, a list of evidence in the folder appears.

2. In the list, for each evidence file that you want to add to another folder, select the check box to the left of the evidence title.

3. Above the evidence list, click **Add to Folder**.

4. On the dialog box, in the **Select Folder** list, click the folder you that you want to add the evidence to, and then click **Select**.

5. On the confirmation message box, click **OK**.

   Evidence.com adds the evidence to the folder that you selected.

6. If you want to confirm that the evidence is in the folder that you added to, below the case ID, click the folder and view the evidence list.

**Remove Evidence from a Folder**

You can remove evidence from any evidence folder, as needed. The exception is the All Evidence folder; you can never remove evidence from the All Evidence folder.

If you need to remove evidence from a case, see Remove Evidence from a Case.

1. On the View Case page, click the evidence folder from which you want to remove evidence.
Below the evidence preview area, a list of evidence in the folder appears.

2. In the list, for each evidence file that you want to remove from the folder, select the check box to the left of the evidence title.

3. Above the evidence list, click Remove from Folder.

4. On the confirmation message box, click Remove.

5. On the message box, click OK.

   Evidence.com removes the selected evidence from the folder. The evidence remains in the case.

---

**Work with Evidence in a Case**

For evidence that is in a case, you can perform the actions described in this section.

---

### Preview Evidence in a Case

From the View Case page, you can view evidence that is in the case. Preview is only available for some of the supported evidence file types.

1. On the View Case page, click an evidence folder that the evidence is in.

   Below the evidence preview area, a list of evidence in the case appears.

2. In the list, find the evidence that you want to preview and then click the evidence title.

   If the evidence file type is supported, the preview area shows the evidence file.

---

### View Evidence from a Case

From a View Case page, you can open the Evidence Detail page for evidence included in the case.

1. On the View Case page, click an evidence folder that the evidence is in.

   Below the evidence preview area, a list of evidence in the case appears.

2. In the list, find the evidence that you want to view and then click the evidence title.

   The Evidence Detail page appears. For more information, see Working with Any Evidence.
Download Evidence from a Case

From a View Case page, you can download evidence files for evidence included in the case.

1. On the View Case page, click an evidence folder that the evidence is in.

   Below the evidence preview area, a list of evidence in the case appears.

2. In the list, find the evidence that you want to download and then click ↓.

   A dialog box shows information about the evidence file.

3. Under Filename, click the evidence file name.

   The download begins. The exact behavior depends on the browser you use and its download settings.

4. Click Close.

View Map

You can view an evidence map that shows the location of evidence in the case, if the evidence has location information. For more information, see Edit Location.

The map icon used for an evidence file is determined by the evidence type. There are six icons that correspond to file types:

- Video
- Audio
- Document
- Image
- Firing Log
- Other
To view an evidence map for a case, on the View Case page, click **View Map**.

### Case Evidence Map Actions

A case evidence map provides basic features for finding and viewing evidence location on the map.

The following table describes the basic actions that are available on the case evidence map.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>See information</td>
<td>1. Click on the icon for the evidence.</td>
</tr>
<tr>
<td>about evidence</td>
<td>- Evidence.com shows information about the evidence.</td>
</tr>
<tr>
<td></td>
<td>2. If you want to see more information about the evidence, click View</td>
</tr>
<tr>
<td></td>
<td>- Evidence.</td>
</tr>
<tr>
<td></td>
<td>- The Evidence Detail page opens.</td>
</tr>
<tr>
<td>Pan</td>
<td>1. Position the mouse pointer over the map.</td>
</tr>
<tr>
<td></td>
<td>2. Click and hold the mouse button.</td>
</tr>
<tr>
<td></td>
<td>3. Move the mouse to pan the map.</td>
</tr>
<tr>
<td></td>
<td>4. Optionally, click <strong>Redo Search in this Area</strong> to see additional</td>
</tr>
<tr>
<td></td>
<td>evidence in the new map view.</td>
</tr>
</tbody>
</table>
### View Case Audit Trail

You can view the audit trail for a case. On the View Case page, the View Audit Trail button appears in the upper-right corner of the page.

1. Click **View Audit Trail**.

   A dialog box shows options for viewing the entire audit trail or a portion of the audit trail.

2. If you want to view the whole audit trail, under **View entire audit trail**, click **Submit**.

3. If you want to view a portion of the audit trail, under **View portion of audit trail**, specify a date in either or both the **From** or **To** boxes and click **Submit**.

   Evidence.com opens or downloads a PDF for the case audit trail. The exact behavior depends on the browser you use and its download settings for PDF files.

4. Save or view the audit trail PDF as needed.

### Sharing Cases Inside and Outside Your Agency

Evidence.com provides three ways to share cases, each allowed or prohibited by a separate permission, enabling administrators to control sharing closely.

#### Share a Case with Other Users in Your Agency

Administrators and users allowed the Case Management “Share” permission can share cases with other users in your agency. Users who you share a case with are **members** of the case. Case members can only access the case after signing in to your Evidence.com agency.

1. Search for the case that you want to share.

2. In the list of cases, find the case that you want to share and then click the ID of the case.
The View Case page appears.

3. Click **Share Entire Case**.

A dialog box presents the three case sharing options.

4. Click **Add Agency Members** and then click **Next**.

The Manage Members dialog box appears.

```
Manage Members
Add members of your agency to this case. Members will have access to this case for the specified number of days.

Enter last name, first name, badge ID, or email address of user to share with

Current Members

<table>
<thead>
<tr>
<th>Name</th>
<th>Badge</th>
<th>Access Beginning</th>
<th>Access Ending</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hamish, MC</td>
<td>MW007</td>
<td>N/A - Owner</td>
<td>N/A - Owner</td>
</tr>
</tbody>
</table>
```

5. For each user who you want to share the case with, start typing the name of the user, wait for Evidence.com to show the matching users, and then click the user you want. You can also type the user badge ID or email address.

Each user you select appears above the box.

6. In the **Shared Duration** box, enter the number of days that the evidence is to be available to the users you are sharing the case with.

7. When you have finished adding all the users with whom you want to share this case, click **Share**.

8. On the confirmation message box, click **OK**.

Evidence.com sends each user an email that invites them to share the case.

**Share a Case by Download Link**

Sharing by download link enables you to share a case and its evidence with anyone who uses the download link during the sharing duration. A download link is a web link that allows anyone with the link and a web browser to access the case and its evidence. This method of
sharing is unauthenticated, that is, downloading the case and its evidence does not require signing in to an Evidence.com agency.

**Note:** It is recommended that, whenever possible, you share cases and evidence using an authenticated sharing method, such as sharing with users in your agency and sharing with partner agencies. This ensures that only the people you intend to grant access to a case and its evidence do receive access.

If you need to share a case with someone who is not a user in your agency or a partner agency, consider using the bulk evidence-sharing feature, which supports sharing with users of my.evidence.com. Anyone with access to email can create an account on my.evidence.com. Evidence you share with a my.evidence.com account is only available to people who know the user credentials for authenticated access to the account. For more information, see Bulk Share Evidence by Authenticated Sharing.

Evidence.com supports the following file types for the case download file:

- **ZIP** — Evidence.com includes the case and its evidence files in a ZIP file.
- **ISO** — Evidence.com includes the case and its evidence files in an ISO image, which can be used to create a CD-ROM or DVD.

Administrators and users allowed the Case Management “Share External Download Links” permission can share cases by download link.

1. Search for the case that you want to share.

2. In the list of cases, find the case that you want to share and then click the ID of the case. The View Case page appears.

3. Click **Share Entire Case**.

   A dialog box presents the three case sharing options.

4. Click **Send Download Link** and then click **Next**.

   The Send Download Link dialog box appears.
5. Use the first box to add the people with whom you want to share the case and its evidence, as follows:

- For a user in your agency or a partner agency, start typing the name of the user, wait for Evidence.com to show the matching users, and then click the user you want. You can also type the user badge ID or email address.

  The user you selected appears above the box. If the user is in your agency, the user has a white background. If the user is in a partner agency, the user has a green background.

- For a person who is not a user in your agency or in a partner agency, type the email address of the person and then press **Enter**.

  If the person already has a my.evidence.com account, the email address appears above the box, with a yellow background.

  If the person does not have a my.evidence.com account, the email address remains in the first box. The person receives an email with the download link; however, if you need to add more users, complete this procedure, and then repeat it until you have shared the evidence with all required users.

6. In the **Shared Duration** box, type the number of days that the case is to be available for download.

7. If you want to include audit trails, check the corresponding check box.
8. Under **Select Package Type**, select the file type that you want for the download file.

9. Click **Share**.

10. On the notification message box, click **OK**.

   Each recipient you specified receives an email that includes the link for downloading the evidence.

   Evidence.com makes the case and its evidence available for download, until the sharing duration expires.

**Share a Case with a Partner Agency**

Evidence.com makes it easy to share cases and their evidence to organizations such as City and District Attorneys. After you have added the evidence, you share the case with the trusted partner agencies that you choose.

Administrators and users allowed the Case Management “Share with Partner Agencies” permission can share cases with partner agencies.

When you share a case with a partner agency, Evidence.com sends the partner agency a copy of the files, which they can manage independently, with no effect on your case and its evidence.

**Note:** If you want to allow users in a partner agency to have only temporary access to evidence, consider bulk sharing the evidence rather than sharing the case. For more information, see Bulk Share Evidence by Authenticated Sharing.

Evidence.com copies the metadata applied to the case, too. For more information, see Receiving Shared Cases from Partner Agencies.

After Evidence.com finishes copying the case to receiving agencies, Evidence.com notifies the recipients that the shared case is available. Recipients can begin managing the case as needed.

1. Search for the case that you want to share.

2. In the list of cases, find the case that you want to share and then click the ID of the case.

   The View Case page appears.

3. Click **Share Entire Case**.

   A dialog box presents the three case sharing options.

4. Click **Share With Partner Agency** and then click **Next**.
The Share with Partner Agency dialog box appears.

5. Use the first box to add the users or groups of the partner agency with whom you want to share the case, as follows:

- To share with a user in a partner agency, start typing the name of the user, wait for Evidence.com to show the matching users, and then click the user you want. You can also type the user badge ID or email address.

  The user you selected appears above the box.

- To share with a group in a partner agency, start typing the name of the agency, wait for Evidence.com to show the available groups of matching agencies, and then click the group you want.

  The group you selected appears above the box.

If you add the wrong user or group, you can remove it by clicking the \( \times \) at the right end of the user or group name.

6. In the Inv
de Expiration box, type the number of days that the invitation to share the case is valid.

7. Under Include, select the check boxes for the additional information that you want to give to the partner agencies you are sharing with.
8. In the **Optional Message to Recipient(s)** box, type any useful or required message, as needed.

9. If you want to review the evidence that you are sharing, under **Case Evidence**, view the evidence list. Scroll down as needed. If you want to view evidence in a new browser window, click the evidence title.

10. Click **Share** and then, on the confirmation message box, click **OK**.

Evidence.com copies to the partner agency the case, its evidence, and any of the additional information you included. After the copy is complete, Evidence.com emails the users and group members with whom you shared the case, notifying them that the shared case is available.

### Update Partner Agency When Adding Evidence

When you add evidence to a case that you have shared with a partner agency, Evidence.com prompts you to update the partner agencies. If the Share with listed Partner(s) check box is selected, Evidence.com send invites to all of the agencies you have previously shared with to accept the newly added evidence.

For more information, see Add Evidence to a Case.

### Update Partner Agencies from the Case Members Page

The Partners list, available on the View Case page after you click View Members, displays the partner agencies that the case is shared with, including whether each partner agency’s copy of the case is up to date.

If a partner agency status is “Out of Date”, the partner agency’s copy of the case is missing evidence. You can share the evidence that the partner agency is missing by selecting Update.

For more information, see View, Update, Add, and Remove Members.

### View, Update, Add, and Remove Members

When you want to know who has access to a case, you can view lists of users and partner agencies with whom the case is shared.

Case members are the users who have access to the case, including the case owner. Additionally, partner agencies with whom a case is shared are also considered members.

1. On the View Case page, click **View Members**.

   Evidence.com shows a list of users in your agency who have access to the case. The case owner is listed first. Users with whom the case is shared are listed below the owner.
If the case is shared with partner agencies, they are listed below the list of users.

2. Take any additional actions that you need. The following table provides information about the available actions.

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a user</td>
<td><strong>Note:</strong> It is recommended that you add members to a case by following the steps in Share a Case with Other Users in Your Agency.</td>
</tr>
<tr>
<td></td>
<td>1. Above the list of users, click Add Member.</td>
</tr>
<tr>
<td></td>
<td>2. A user search page appears.</td>
</tr>
<tr>
<td></td>
<td>3. Search for the user you want to add to the case.</td>
</tr>
<tr>
<td></td>
<td>4. To the left of the user name, select the check box.</td>
</tr>
<tr>
<td></td>
<td>5. Above the search results, click Add to Case.</td>
</tr>
<tr>
<td></td>
<td>6. In the Length (In Days) to Share This Case box, type the number of days that the user should have access to the case, and then click OK.</td>
</tr>
<tr>
<td></td>
<td>7. On confirmation message box, click Return to Case.</td>
</tr>
<tr>
<td>Add a partner agency</td>
<td>Perform the steps in Share a Case with a Partner Agency. You cannot add a partner agency from the list of case members.</td>
</tr>
<tr>
<td>Update a partner agency</td>
<td>1. Under Partners, find the agency whose status is “Out of Date”.</td>
</tr>
<tr>
<td></td>
<td>2. To the right of the partner agency name, click Update.</td>
</tr>
<tr>
<td></td>
<td>3. On the notification message box, click OK.</td>
</tr>
<tr>
<td></td>
<td>The status of the partner agency changes to “Awaiting Acceptance”.</td>
</tr>
<tr>
<td></td>
<td>Evidence.com sends the partner agency an invitation to accept the additional evidence.</td>
</tr>
<tr>
<td>View user information</td>
<td>1. Find the user in the list of case members.</td>
</tr>
<tr>
<td></td>
<td>2. Click the user name.</td>
</tr>
<tr>
<td></td>
<td>The User Summary page appears.</td>
</tr>
</tbody>
</table>
### Action Steps

<table>
<thead>
<tr>
<th>Action</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove a user from the case</td>
<td>1. Find the user in the list of case members.</td>
</tr>
<tr>
<td></td>
<td>2. To the right of the user name, click $\times$ (remove member).</td>
</tr>
<tr>
<td></td>
<td>3. On the confirmation message box, click Yes.</td>
</tr>
<tr>
<td></td>
<td>4. On the notification message box, click OK.</td>
</tr>
</tbody>
</table>

### Receiving Shared Cases from Partner Agencies

When a partner agency shares a case with users or groups in your agency, Evidence.com copies the case to your agency first and then sends a notification message to each recipient. No approval or acceptance of the case is required. Because cases shared from a partner agency are a copy of the files, you can manage the case and its evidence independently, with no effect on the case or evidence in the partner agency.

Your agency can manage the case as you would a case that was created in your agency. When Evidence.com copies the case to your agency, assumptions are made regarding case ownership, metadata, and audit trails, as described in the following sections.

### Assignment of Case Ownership

Cases can have only one owner; however, a partner agency can specify more than one user or group in your agency to share a case with. Evidence.com chooses one user to be the case owner. Evidence.com assigns the other users to the case as members.

When it chooses an owner, Evidence.com prioritizes the choice.

1. **Users** — If the case is shared with more than one user or a user and groups, Evidence.com chooses the owner from the users, choosing at random if there is more than one individual user to choose from.
Group monitor — If the case is shared with one or more groups but no individual users, Evidence.com chooses the owner from the monitors of the groups, choosing at random if there is more than one monitor to choose from.

Group member — If the case is shared with one or more groups that have no monitors and is not shared with individual users, Evidence.com chooses the owner from among the members of the groups, choosing at random if there is more than one member to choose from.

Case Metadata

In general, a case shared by a partner agency includes the metadata that the partner agency applied. For some metadata, Evidence.com takes special actions.

- **Case ID** — The ID assigned by the partner agency.
- **Description** — The description assigned by the partner agency.
- **Categories** — None. Evidence.com does not apply a retention category to the case. Evidence.com adds a note to the case to record any retention categories that the partner agency applied to the original case. Because retention policies vary among agencies, Evidence.com does not attempt to determine which of your agency’s retention categories should be applied to a case received from a partner agency.
- **Tags** — The tags applied by the partner agency, with the partner agency name appended. For example, if the partner agency applied the tag “McKinley”, the copy of the case that you receive includes the tag “McKinley (partner agency name)”. The tags are also added as notes to the case, to ensure that there is a record of the tags that were received. You can delete the tags that were copied from the partner agency.
- **Notes** — The notes created by the partner agency, with the partner agency name added. Evidence.com adds notes to record the tags and categories that the partner agency had applied to the original case.

Audit Trails

If the partner agency does not include audit trails in the shared case, the case audit trail in your agency includes only the entries for actions taken in your agency.

If the partner agency includes audit trails in the shared case, the case audit trail in your agency includes all audit trail entries from the partner agency in addition to the entries for actions taken in your agency.
<table>
<thead>
<tr>
<th>#</th>
<th>Date</th>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>89</td>
<td>21 Mar 2016</td>
<td>10:56:21 (-07:00)</td>
<td>Case share copy initiated by Hamish, MC (Badge ID: MCH327, Agency: Police Department) Username: mharmish Case share copy initiated by Hamish, MC (Badge ID: MCH327, Agency: Police Department)</td>
</tr>
<tr>
<td>90</td>
<td>21 Mar 2016</td>
<td>10:56:24 (-07:00)</td>
<td>System</td>
</tr>
<tr>
<td>91</td>
<td>21 Mar 2016</td>
<td>10:55:25 (-07:00)</td>
<td>System</td>
</tr>
<tr>
<td>92</td>
<td>21 Mar 2016</td>
<td>10:57:20 (-07:00)</td>
<td>Carpenteria, Soledad (Badge ID: SC601) Username: sc601 Case or Case Related Record Accessed</td>
</tr>
</tbody>
</table>
Inventory and Device Management

Administrators and users who are allowed the Device Administration permission can manage Axon and TASER devices by using the Inventory menu options.

The Inventory page allows administrators and users with the required permissions to search for, view information about, and manage Axon devices including body worn cameras, CEWs, Signal devices, and Axon Fleet vehicles.

**Note:** If your agency does not use CEWs or Axon Fleet, those search options will not appear on the Inventory page.

From the Inventory page, you can:

- **Search specific device type** – Find and manage Axon body worn cameras, CEWs, Docks, Interview Rooms, and Signal devices.
- **Search Vehicles** – Add, find, and manage Axon Fleet vehicles and their associated devices.
- **Search All Devices** – Find and manage all devices.
- **Bulk Assign** – Allows assignment of up to 10 devices at one time.
- **Make a Return** – Opens the Axon Returns site in a new browser window to let you start the return process or check the status of devices return to Axon.
Device Search — All Devices and CEWs

The search for specific device type or All Devices options provides search features to help you find and manage devices.

1. On the menu bar, click **Inventory**.

2. Click on the device type you want to search for or **All Devices**.

The device search results list with selected devices, sorted by the Last Upload date, is shown.

3. Search for the devices that you need. The following table provides steps for search-related tasks.

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find devices assigned to you or another person.</td>
<td>In the <strong>Assigned To</strong> field, enter the name of person whose devices you want to see.</td>
</tr>
<tr>
<td>Find unassigned devices.</td>
<td>In the <strong>Device Status</strong> filter, select <strong>In Stock</strong>.</td>
</tr>
<tr>
<td>Change search results</td>
<td>Update the device search filters or click <strong>Reset Filters</strong>. For more information, see <a href="#">Device Search Filters</a>.</td>
</tr>
<tr>
<td>Sort search results</td>
<td>Use the <strong>Sort By</strong> list to select a column and click <strong>Sort Order</strong> to change order. Click the column heading for <strong>Serial Number, Device Name, Last Upload, Device Status, Error Status, Firmware, or Warranty</strong>. To reverse the sort order, click the heading again.</td>
</tr>
</tbody>
</table>

For information about the actions you can take from search results, see [Working with Device Search Results](#).
Device Search Filters

Device search filters help you limit search results to the devices that you want to see. The search results only include devices that match all the search filters that you set.

**Basic Search Filters**

- **Serial Number** — Limits search results to devices whose assigned serial number includes the characters entered in this field. This filter supports partial matches. For example, if you entered \textit{X81}, the search results would include devices with the serial numbers \textit{X81162367} and \textit{X81233704}.

- **Device Name** — Limits search results to devices whose name includes the characters entered in the Device Name field. By default, device names are the same as the device serial number; however, agencies can assign custom device names to some devices, such as body worn cameras and CEWs. This filter supports partial matches.

- **Assigned To** — Limits the search to devices that were most currently assigned to the specified user. Users can enter their name to see devices assigned to them.

- **Upload Date Start** — Limits search results to devices that uploaded to Evidence.com between the set dates. You can specify a date and time range by using the Start and End fields, otherwise the search is not limited by date range. Search results are inclusive of the dates specified.
  
  - **Start** — The start of the date and time range. If the Start field is empty, the date range begins with the earliest possible date.
  
  - **End** — The end of the date and time range. If the End field is empty, the date range ends with today.

**Advanced Search Filters:** Click Show Advanced Search to show these additional search filters.

- **Device Model** — Limits the search results to specified device model.

- **Device Status** — Limits the search results to devices with the specified status. To search for unassigned devices, select \textbf{In Stock} in the Device Status filter.

- **Error Status** — Limits the search results to devices with the specified error status.

The results of the search are shown below the search filters. Use the **Sort By** list to select a column and click **Sort Order** to change order. Alternately, you can click the column heading
for **Serial Number**, **Device Name**, **Last Upload**, **Device Status**, **Error Status**, **Firmware**, or **Warranty** to change the sort by column. To reverse the sort order, click the heading again.

## Working with Device Search Results

On device search page, you can take the actions described in this section.

![Device Search Results](image)

### Update Device Status

Users with Device Administration permission change the status, including unassigning devices, for selected devices. Most Axon devices can also be assigned and unassigned using the Axon Device Manager app.

1. Search for the device or devices.
2. Select the devices in the search results
3. Click **Update Status** and selects the new status from the list.
Devices can be unassigned by changing the device status to In Stock. Devices cannot be assigned using Update Status. Devices can be assigned using Axon Device Manager or on the Device Profile page or by using the Bulk Assign option.

4. Click **Update** to save the changes.

The device status is updated. Click **Close** to continue.

### Device Status Descriptions

The following table provides a description of the different device statuses.

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>In Stock</td>
<td>This device has been registered to your agency, but not assigned to a user.</td>
</tr>
<tr>
<td>Assigned</td>
<td>This device has been assigned to a user in your agency.</td>
</tr>
<tr>
<td>Review</td>
<td>This device is registered to your agency and is currently undergoing investigation/troubleshooting.</td>
</tr>
<tr>
<td>RMA</td>
<td>This device is registered to your agency and has been returned to Axon for RMA processing.</td>
</tr>
<tr>
<td>Relinquished</td>
<td>This device was registered to your agency, was returned to Axon, and is no longer registered with your agency. The device remains in your search list for historical and audit purposes.</td>
</tr>
<tr>
<td>Lost</td>
<td>This device is registered to your agency and has been reported as lost.</td>
</tr>
<tr>
<td>Stolen</td>
<td>This device is registered to your agency and has been reported as stolen.</td>
</tr>
<tr>
<td>Scrapped</td>
<td>This device is registered to your agency and has been reported as destroyed or no longer serviceable.</td>
</tr>
<tr>
<td>In Evidence</td>
<td>This device is registered to your agency and is being held as physical evidence and has been withdrawn from deployment.</td>
</tr>
</tbody>
</table>
View Device Profile

1. Search for the device you want to view.

2. In the search results, click the serial number of the device.

The Device Profile page opens.

By default, the Summary tab is selected. The Summary tab shows essential information about the device, such as the firmware version and warranty information. It also provides access to the device audit trail.

For body worn cameras, the Summary tab also includes information about the most recent Axon Dock connection for the Axon camera. This information can be used to help locate the current, or last known, Axon Dock by providing the name and serial number of the Dock, in addition to showing when the camera last communicated with Evidence.com. Additionally, it shows if the device is currently uploading videos to Evidence.com.

For CEWs, an Event Info tab is included on the Device Profile page. This tab displays the firing log information of the device.

For information about the actions you can take from the Device Profile page, see Working with a Device.
View Device Assignee

From device search results, you can view information about the user to whom a device was most recently assigned.

1. Search for the device whose assignee you want to view.

2. In the search results, find the device and then, under **Assignee**, click the user's name.

   The User Summary page displays information about the user to whom the device was most recently assigned.

   For information about actions available from the User Summary page, see User Administration.

Export Device Search Results

You can export the results of a device search in PDF, text, or Microsoft Excel/CSV format.

**Note:** When device search results are exported in Microsoft Excel or CSV format, the Device Assignee First Name and Last Name are split into separate columns and a Badge ID column is included.

If the search results contain more than 500 devices, Evidence.com exports the search results in 500-device segments and asks you to confirm the download of the next segment.

1. Search for devices and refine the search until the search results represent the device list that you want to export.

2. Above the search results, click **Export**.

3. In the **Select Format** list, click the file format that you want for the exported device-search results and then, on the message box, click **Export**.

   The device search results download in the format that you specified.

   If the device search results contain more than 500 devices, only the first 500 devices are included in the downloaded file and Evidence.com displays a dialog box for downloading the next 500 devices in the search results.

4. If you want to export device search results for additional devices, click **OK** each time the dialog box appears.

   The device search results download in a separate file for each 500-device segment of the search results.
Working with a Device

This section describes the actions available on the Device Profile page.

**Edit Device Settings**

The device settings that can be changed depend on the type of device and agency level device settings.

- For Axon Flex cameras, you can edit the device name and orientation.
- For Axon Body 2 cameras, you can edit the device name, configure the speaker volume, configure camera vibration, camera indicator lights, and whether the camera is in stealth mode.
- For Axon Flex 2 cameras, you can edit the device name, orientation, configure the speaker volume, configure controller vibration, indicator lights, and whether the camera is in stealth mode.
- For other device types, you can change the device name.

1. On the Device Profile page, click the **Settings** tab.
2. Edit the settings as needed.
3. Click **Save Settings**.

**Assign a Device**

For most device types, you can use the Device Profile page to assign the device to a user.

**Note:** Devices can also be assigned using Axon Device Manager or using the Bulk Assign option.

1. On the Device Profile page, click the **Assign Device** tab.
2. In the **Assign Device To** box, start typing the name of the user who you want to assign the device to, wait for Evidence.com to show the matching users, and then click the user you want. You can also type the user badge ID.
3. Click **Assign Device**.

Evidence.com assigns the device to the user you selected.
View Evidence Created by a Device

Any evidence recorded on the device that has been uploaded to Evidence.com appears on the Device Evidence tab.

1. On the Device Profile page, click the **Device Evidence** tab.

   Evidence.com shows a list of all evidence uploaded from the device.

2. Use the evidence list as needed. The following table provides concise steps for the tasks you can perform from the evidence list.

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Add evidence ID             | When evidence does not have an ID assigned, “Add” appears in the ID column. If you want to add an ID to evidence:  
                                1. In the ID column, click **Add**.  
                                A dialog box appears.  
                                2. In the **Enter ID** box, enter the ID that you want to assign to the evidence, and then click **Save**. |
| View evidence               | In the **Title** column, click the title of the evidence. The Evidence Detail page displays information about the evidence. For more information about actions available from the Evidence Detail page, see Working with Any Evidence. |
| View evidence owner         | In the **Owner** column, click the name of the evidence owner. The User Summary page displays information about the user. |
| View evidence audit trail   | In the **Actions** column, click **>Add**. For more information, see View Evidence Audit Trail. |
| Download evidence file      | In the **Actions** column, click **Download**. For more information, see Download Evidence File. |
| Flag or un-flag evidence    | In the **Actions** column, click **Flag or Un-Flag**. For more information, see Flag or Un-Flag Evidence. |

Device Audit Trail Information

All Axon and TASER device audit trails show events and changes for the selected device. The audit information can be filtered to a particular date range or show the entire life of the device.

The audit information is available in both PDF and comma-separated values (CSV) format, with each event, action, or change shown on a different line in the audit trail.

- The PDF file has four columns: Item, Date/Time, Event, and Additional Information. The Item column is a numerical listing of the events, actions, or changes for this file and item number will change depending on the selected date range for the audit trail. The Event column has a short description of the event, action, or change. The
Additional Information column has general camera status information such as remaining battery %, video count, MB remaining, and firmware version.

- The CSV file has seven columns: Date Time, Action, Battery %, Video Count, Firmware Version, MB Remaining, and Unique ID. The Action column has a short description of the event, action, or change and corresponds to the PDF Event column. The Battery %, Video Count, Firmware Version, and MB Remaining columns have camera status information and correspond to the information shown in the PDF Additional Information column. The Evidence UID column is a unique string that is generated for all pieces of evidence on Evidence.com.

The following events and changes appear in the audit trail for all devices:

- Device registration
- Device status changes
- Device assignment information
- Device metadata changes

For Axon Body 2 and Flex 2 cameras, the following events, actions, and changes appear in the audit trail:

**Note:** For Axon Body 2 and Flex 2 cameras with v1.7 or earlier firmware release, only the camera registration, status change, and assignment information is available. The other events listed are available with the v1.8 or later firmware release for Axon Body 2 and Flex 2 cameras.

- Camera registered
- Camera status change
- Power on or off
- Event button press or hold
- Recording start or end
- Audio recording disabled or enabled
- Camera docked or undocked
- Video accessed or streamed using Axon View or Evidence Sync
- Category updated using Axon View or Evidence Sync
- ID updated using Axon View or Evidence Sync
• Title updated using Axon View or Evidence Sync
• Function button press or hold
• Battery status button press or hold
• Volume mute, low, medium, or high
• Stealth mode enabled or disabled
• Indicator lights enabled or disabled
• Marker added
• GPS coordinates added
• Date/Time Sync
• Camera assignment
• Firmware updated

Get a Device Audit Trail

1. On the menu bar, click Inventory.
2. Search for the device you want to view.
3. In the device search results, click the device Serial No.
   The Device Summary page is shown.
4. Click Audit Trail.

   A dialog box with options selecting for the date range and file type is shown.
5. Under Select Date Range, do one of the following:
   • If you want to view the entire audit trail for the life of the device, select View entire audit trail.
   • If you want to view a portion of the audit trail, select View portion of audit trail and then specify a date in either or both the From or To boxes or click a shortcut for a date range, such as Yesterday.
6. Under Select File Type, click the file type, CSV or PDF, that you want.
7. Click Submit.
Evidence.com generates and downloads the audit trail in the format you selected.

8. Save or view the audit trail file, as needed.

**Vehicle Search**

The Vehicle search section allows administrators and users with the correct permissions to add, find, and manage Axon Fleet vehicles and their associated devices.

The Vehicle section only available to agencies that use Axon Fleet.

**Add One New Vehicle**

Vehicle information must be configured in Evidence.com before Axon View XL can connect to Evidence.com and before videos can be uploaded from Fleet Cameras. The mobile data terminal (MDT) or mobile digital computer (MDC) in the vehicle uses the SSID information to connect to Evidence.com.

1. On the Inventory page, click **Vehicles**.

   The vehicle page displays a list of vehicles with Axon Fleet systems associated with your Evidence.com account.

2. Click **Create Vehicle**.

3. Type a Name for the vehicle and click **Save and Continue**.

![Add One New Vehicle Diagram]
4. Enter the serial number for Axon Signal Vehicle associated with the vehicle and click **Save and Continue**.

**Note:** The serial number for Axon Signal Vehicle always begins with X87.

5. Enter the serial numbers for the Axon Fleet Power Units associated with the Fleet Camera front and back mounts, and the click **Save and Continue**.
6. Enter the SSID and Password for the vehicle and then click Save and Continue.

The SSID is used by the vehicle's MDT or MDC to connect to Evidence.com.

7. Select if wireless offload for the Fleet Cameras is enabled for the vehicle by moving the corresponding switch to the right.

Note: If wireless offload is not enabled, then the Fleet Cameras must be manually removed from the vehicle and docked to upload videos to Evidence.com.

8. Click Save and Complete.

9. If you need to add another vehicle, click Add Another and repeat steps 3 – 8.
Add Multiple New Vehicles

This option allows users to add information for multiple Axon Fleet 2 and Axon Fleet vehicles at one time using a comma-separated values (csv) file.

The csv file requires the same information as when creating a single vehicle. The csv file has seven columns and the first row must contain the header information for the file. The following image shows an example csv file layout.

<table>
<thead>
<tr>
<th>Vehicle Name</th>
<th>Signal</th>
<th>Front Mount</th>
<th>Rear Mount</th>
<th>SSID</th>
<th>Password</th>
<th>Wireless Offload</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID444</td>
<td>X87000025</td>
<td>X850000022</td>
<td>X850000023</td>
<td>garage-a</td>
<td>arc-2343x9</td>
<td></td>
</tr>
<tr>
<td>ID447</td>
<td>X87000026</td>
<td>X850000024</td>
<td>X850000025</td>
<td>garage-a</td>
<td>arc-2343x9</td>
<td>TRUE</td>
</tr>
<tr>
<td>ID449</td>
<td>X87000027</td>
<td>X850000026</td>
<td>X850000027</td>
<td>garage-a</td>
<td>arc-2343x9</td>
<td>FALSE</td>
</tr>
</tbody>
</table>

Each heading and the expected information is listed below.

- **Vehicle Name**: A unique name for the vehicle.
- **Signal**: The serial number for the Axon Signal Vehicle unit for the vehicle. This serial number always begins with X87.
- **Front Mount**: The serial number for the Axon Fleet Power Unit connected to the front camera. This serial number always begins with X85.
- **Rear Mount**: The serial number for the Axon Fleet Power Unit connected to the rear camera. This serial number always begins with X85.
- **SSID**: The Service Set Identifier (SSID) for the network used by the vehicle.
- **Password**: The network password.
- **Wireless Offload**: Sets if the vehicle will use wireless offload. Use TRUE to enable wireless offload for the vehicle. Use FALSE or leave blank if wireless offload is disabled for the vehicle.

1. On the Inventory page, click **Vehicles**.

   The vehicle page displays a list of vehicles with Axon Fleet systems associated with your Evidence.com account.
2. Click **Bulk Creation**.

The Bulk Vehicle Import page is shown. From this page you can download the template used for bulk vehicle creation and upload the vehicle csv files.

Click **Download Template** to download a copy of the template with dummy data. Delete the dummy vehicle information (row 2) before uploading the csv file.

3. Upload the csv file by dragging it onto the page or by clicking **Choose File** and selecting the file from a saved location.

The csv file is uploaded to Evidence.com.

4. After the csv file is uploaded, you are asked to review the vehicle information. If any of the vehicle information is incorrect, you can click on the incorrect entry to edit it. You can delete a vehicle row by clicking the delete (trash can image) icon.
Once you have confirmed all the information is correct, click **Create** to create the new vehicles.

### Edit Vehicle Information

1. On the Inventory page, click **Vehicles**.

   The vehicle page displays a list of vehicles with Axon Fleet systems associated with your Evidence.com account.

2. Find the vehicle you want to edit in the list and click on the vehicle name.

   You can use the Vehicle search field to narrow the list of vehicles shown in the list.

3. On the vehicle page, click the edit icon (EDIT) on the same line as the information you want to change.

4. Enter the updated information and click **Save and Continue** (or **Save and Complete**).

   If needed, edit the next set of information.

   Once all edits are completed, you can go to any other Evidence.com page.

### Bulk Assign Devices

Using the Bulk Assignment feature, you can assign multiple devices at one time.

1. On the menu bar, click **Inventory**.
2. On the Inventory page, click **Bulk Assign**.

   The Bulk Assign page appears.

3. In the first field under **Owner**, start typing the name of the user who you want to assign the device to, wait for Evidence.com to show the matching users, and then click the user you want. You can also type the user badge ID.

4. In the same row under **Serial no.**, start typing the serial number of the device that you want to assign to the owner, wait for Evidence.com to show the matching devices, and then click the device that you want to assign.
5. For each additional device that you need to assign, repeat the previous two steps in a new row. If you need more rows, click **Add More Rows**.

   You can have a maximum of ten rows.

6. When you are done specifying users and the devices to assign to them, click **Assign Devices**.

   A notification message box appears.

7. Click **OK**.

   Evidence.com assigns the devices to the users that you specified.

8. To verify that the devices are correctly assigned, use the All Devices page to search for each device by serial number or assigned to and then confirm the correct assignment in the search results.

### Axon Device Manager

The Axon Device Manager app simplifies and accelerates device assignment of Axon devices, such as Axon Body 2 and Axon Flex 2 cameras. Axon Device Manager runs on Android devices that are equipped with an NFC antenna and iOS devices.

With the app running, the armorer taps the iOS or Android device on the back of the Axon device to receive the device type and serial number. The armorer then searches for and selects an Evidence.com user, and assignment is complete. The entire process takes only seconds per Axon device.

You can find out more about Axon Device Manager in the [Axon Help Center](#).
Reporting

Evidence.com allows administrators and those with the reporting permission to generate reports showing Evidence.com utilization. These options can help your agency turn that data into valuable answers to ensure your Evidence.com account is providing you with the flexibility and utility your agency deserves.

Evidence.com reports are spreadsheets that can be opened by many spreadsheet applications. Reports include all relevant metadata for the items included in the report. Using the Microsoft Excel pivot table function, you can group evidence by any of the fields, such as owner or badge ID, to get a better understanding of individual officer usage or certain category retentions over a given period. For more information, see Example Data Aggregation Using Microsoft Excel Pivot Tables.

The reports available are the following:

- **Evidence Created** — Lists all evidence on your agency’s account in order of when the data was created. It also lists all associated metadata attached to those pieces of evidence and shows the number of days between when a piece of evidence was recorded and when it was uploaded to Evidence.com.

- **Evidence Deleted** — Lists all evidence deleted, the associated metadata, and shows the number of days between when a piece of evidence was recorded and when it was uploaded to Evidence.com for your agency’s account, in order of when the data was deleted. This report provides better monitoring of automated deletions and help ensure a proper retention policy is in place.

- **Category Summary** — Lists the current count of total files and file size in megabytes (MB) for each category as well as the percent of files assigned to that category.

- **Uncategorized Evidence** — Lists users with uncategorized evidence assigned to them. A second tab on the export lists every piece of uncategorized evidence and includes the owner information, evidence title, date recorded, and link to the evidence.

- **User Summary** — Lists total files and file size in MB, broken out by owner of the evidence. The counts are further broken out by evidence type, active, and deleted evidence. The report also includes the user’s Last Login Date, Invited Date (This information does not change once the user creates their Evidence.com account, even if the user is deactivated and reactivated), and Deactivated Date (information only appears in this report column if the user has an Inactive status in the system).

- **Axon Video Summary** — Lists usage metrics on Axon videos uploaded to your agency. The first tab is a summary of Number of videos, hours, and MB uploaded. The second tab breaks out the uploads by the specified grouping: Day, Month, or Year.
• **Sharing Audit Report** — Lists all user actions related to sharing evidence and cases. Included in the report are details such as the following examples:
  o Date and time of sharing event
  o Who initiated the sharing event
  o What was shared – evidence or a case
  o How was it shared – internal or external to your Evidence.com agency
  o The ID of the evidence or case shared
  o The recipient of the shared evidence or case
  o The permissions shared to the recipient

• **Device Summary Report** – List information on all the devices (body cameras and CEWs) belonging to your agency. The report includes the following information for each device:
  o Device model, name, and serial number
  o Device status
  o First name, last name, and badge ID of assigned user
  o Firmware version
  o Last upload date/time
  o Body Camera Device Settings (Speaker volume, Vibration, Indicator Lights, and Stealth)
  o Error Status

---

**Run a Report**

You can run any of the reports as needed. A report can take minutes to several hours to generate, depending on the size of the report.

To run a report, you must be allowed the Generate Reports permission, under the Admin Access permissions; however, this permission is dependent on being allowed Any Evidence for the View permission, under the Evidence Management permissions.

1. On the menu bar, click **Reports**.
The Reports page lists the available report types. The Create Report section shows a summary of the selections you make before you run the report. The Download Queue lists the completed reports that are available for download.

2. Under **Select a Report Type**, click the report that you want to run. Depending on the report type, additional report options appear.

3. If the Select A Summary Type report options appears, do one of the following:
   - If you want a User Summary report for all users, click **All Users**.
   - If you want a User Summary report for one user only, click **Single User** and then in the **Reassign To** box, start typing the name of the user, wait for Evidence.com to show the matching users, and then click the user you want.

4. If the Select a Date Range report options appear and you want to change the date range, do one of the following:
   - If you want to use a standard date range, click the link for the date range you want.
   - If you want to set a custom date range, in the From and To boxes, type the dates or click the calendar icon and choose the dates.

5. If the Filter report options appear, click the grouping option that you want.

6. Under Create Report, verify that the report configuration is what you want. If not, modify the report options.

7. Click **Run Report**.

   Under Download Queue, the report is listed, as either Running, Failed, or Download.
When the report is ready, Evidence.com sends you a notification email that includes a download link.

8. If the report status is Download, click **Download**.

## Downloading Reports

You can download reports either by visiting the Reports page or by the download link in a notification email. The Reports page Download Queue lists the last 10 reports you requested.

### Download Report from Reports Page

Completed reports are available from the Download Queue section of the Reports page. If you have permissions to run reports, you can download reports that any user has run.

1. On the menu bar, click **Reports**.

2. Under **Download Queue**, find the report and click **Download**.

    Evidence.com opens or downloads the report spreadsheet file. The exact behavior depends on the browser you use and its download settings for files.

### Download Report from Email Download Link

When a report that you run is complete, Evidence.com sends you a notification email that includes a link for downloading the report. Any user with permission to run reports can use the download link.

1. In a report notification email, click the download link.

    A web browser opens your Evidence.com agency.

2. If the sign-in page appears, enter your Evidence.com credentials and click **Sign In**.

    Evidence.com opens or downloads the report spreadsheet file. The exact behavior depends on the browser you use and its download settings for files.

## Example Data Aggregation Using Microsoft Excel Pivot Tables

This powerful tool allows you to group data by entry types and obtain valuable insight from the large list of detailed entries in the reports. A simple and easy to follow tutorial is available at [http://www.excel-easy.com/data-analysis/pivot-tables.html](http://www.excel-easy.com/data-analysis/pivot-tables.html).

Some examples of what this tool lets you discover:
- Ranking of officers based on usage—Group by officer last name or badge ID and sort by the sum of size or duration.

- Amount of data in each category—Sort out all deleted evidence and group by category. Then sort this data by the sum of size or duration.

- What evidence has been viewed the most—Sort view counts in descending order.
Administrator Overview

The Evidence.com Admin section is used to administer your agency’s Evidence.com account. There are four basic areas, Users, Devices, Agency Settings, and Security Settings. Each basic area has related features for maintaining your account. The features available to you in Evidence.com depends on the permissions granted to your role and the features that are available to your agency.

User Administration

An administrator or a user allowed the User Administration permission generates all user accounts in your Evidence.com agency. When you add a user to your Evidence.com agency, Evidence.com sends an invitation to the email address of the user.

Please note the following requirements and best practices:

- All users in your Evidence.com agency must have unique email accounts.
- Users must have access to their email accounts.
- Each user should have a unique Evidence.com account. It is recommended that you prohibit users from sharing an Evidence.com user account.
- If you do not want to allow users to change their username, email address, or other information, ensure that the role that you assign to users prohibits the Edit Account Information permission.

Note: The default permissions assigned to the User role does allow the Edit Account Information permission. For more information about permissions in pre-configured user roles, see Appendix A: Roles and Permissions.

- Invitations to register with Evidence.com are valid for seven days. If the user fails to register within that span of time, an administrator must re-invite them.
- In order to avoid complications later, it is recommended that you create a policy that dictates username format.

After users have registered in Evidence.com, they can log in to Evidence.com.
User Account Statuses

An Evidence.com user account can have one of the following possible statuses.

- **Active** — The user can access your Evidence.com agency, as determined by the role that you assigned to the user account. Administrators can change user account information for Active users.

  Evidence.com does not permit users who have not completed the registration process to access your Evidence.com agency.

- **Invited** — Active users who have not completed the registration process are considered to have a status of Active/Invited. In user search results, the status of these users is listed as Invited.

- **Password Reset** — Active users whose credentials have been reset by an administrator have a status of Active/Password Reset. In user search results, the status of these users is listed as Password Reset.

- **Inactive** — The user cannot access your Evidence.com agency. Administrators cannot change user account information for Inactive users; however, the audit trails of inactive users remain available.

  Administrators can create user accounts that are Inactive. This enables agencies to pre-provision user accounts with device assignments and other settings, without prematurely allowing the users access to their Evidence.com agency.

  The following figure shows user search results that contain user accounts in each of the possible statuses, as shown by the far right column.

  ![User Account Statuses Table](image)

  You cannot delete user accounts. This ensures that user audit trails are available for any user account that has had access to your Evidence.com agency.

A new user account can be either Active or Inactive. Administrators can deactivate and reactivate user accounts.
**User Account Added as Active**

The following figure shows the basic lifecycle of a user account that is added in the Active state. Until the user registers, the account is in the Active/Invited state.

![User Account Added as Active Diagram]

**User Account Added as Inactive**

The following figure shows the progression of states from Inactive to Active when a user is added in the Inactive state.

![User Account Added as Inactive Diagram]

**Active User Account During Password Reset**

The following figure shows the progression of states between Active and Active/Password Reset.

![Active User Account During Password Reset Diagram]

**Add Users**

You can add users one at a time or many at a time.

A user that you add has the status that you assign: Active or Inactive.
When you add a user with an *Active* status, Evidence.com emails to the user an invitation to join your Evidence.com agency. Invitations to join Evidence.com expire within 7 days. After an invitation expires, an agency administrator can re-invite the user.

When you add a user with an *Inactive* status, the user does not have access to your Evidence.com agency and does not receive notification that you created the user account. Evidence.com allows you to assign devices to an Inactive user and add Inactive users to groups.

### Add One User

When you want to add one user to your agency, use the Add User feature.

1. On the menu bar, click **Admin** and then under **Users**, click **Add User**.

   The Add User page appears.

2. In the following boxes, type the required information.
   
   - **First Name** — The user’s first name.
   - **Last Name** — The user’s last name.
   - **Email Address** — The unique Internet email address of the user.
   - **External ID** — A unique value, assigned by your organization, that identifies the user. If you do not assign a value, Evidence.com will automatically generate one. It is recommended that you determine a user ID strategy that best suits your needs.
   - **Username** — A unique username that you assign.
   - **Badge ID** — A unique badge ID that you assign. Typically, a user’s badge number in Evidence.com should match the user’s badge in other systems such as computer-aided dispatch (CAD) systems. This practice simplifies analysis and reporting of data aggregated from multiple systems. It also simplifies Evidence.com integration with your CAD system.

3. In the **User Role** list, select the role that you want to assign to the user.

4. In the **Status** list, click the status that you want to the user.
   
   - **Active** — The user is able to register and sign in to Evidence.com immediately after you finish adding the user.
   - **Inactive** — The user is not able to register or sign in to Evidence.com.

5. Click **Add**.
Evidence.com adds the user. If the user status is Active, Evidence.com sends the user an invitation email.

A notification message box appears.

6. On the message box, click the button for the action you want to take next.

**Add Many Users**

When you need to add many users to your Evidence.com agency, use the Import Users feature. This feature lets you create many user accounts quickly. You specify details about the new users in a file that you upload to Evidence.com.

You are limited to assigning the same user role to each user that you add from an uploaded file; therefore, create upload files that contain only users that you want to assign to the same user role. For example, create an upload file for users that you want to assign the Armorer role and create a different upload file for users that you want to assign the User role.

The supported file formats are the following formats:

- Comma-separated values (CSV) file — Supported by spreadsheet applications, such as Microsoft Excel.
- Text (TXT) file — Supported by text editors and word processors. It is recommended that you use a text editor such as Microsoft Notepad to ensure that the file format is correct.

In either format, you specify the following information for each user:

- First name
- Last name
- Email address
- Badge ID
- Username
- Status
- External ID (optional – if not provided, Evidence.com will automatically generate one)

**Note:** In order to complete the registration process, users must have access to the email addresses that you specify.

1. On the menu bar, click **Admin** and then under **Users**, click **Import Users**.

   The Import Users page appears.
2. Download the example file for the format that you want to use.

3. Make a copy of the example file and assign it a meaningful file name.

4. Open the file in the appropriate application. For a .txt file, use a text editor. For a .csv file, use a spreadsheet application.

   The first row or line of the file contains column names. The second and third row or line is an example.

   ![Example Table]

5. Delete the second and third lines. Do not delete the first line. Evidence.com expects the first line to contain the column names.

6. For every user that you want to add, include a line in the file that specifies values for the user first name, last name, email address, badge ID, Username, and status. You can include an external ID, but this value is not required.

   Ensure that you separate the values in each row or line appropriately:
   - In a .txt file, ensure that you add a tab after each value.
   - In a .csv file, ensure that each value is in the cell beneath the applicable header.

7. Save the file.

8. In Evidence.com, if your session has timed out, sign in again and return to the Import Users page by clicking Admin and then, under Users, clicking Import Users.

9. Click Choose File and, in the dialog box that opens, select the file on your computer, and then click Next.

   Evidence.com displays a list of the users found in the uploaded file.

10. For each user that you want to add, select the check box to the left of the user first name.

11. In the Role for all users list, click the user role that you want to assign to each user that you selected and then click Next.
Evidence.com displays a confirmation page. The role to be assigned to each user is noted near the bottom of the page.

**12.** Review the user information a final time and then click **Next**.

Evidence.com imports the users and sends each user an invitation email.

A message box displays buttons for importing more users or ending the process.

**13.** Click the button for the action you want to take next.

### Complete the User Registration Process

In order to access your Evidence.com agency, users who have received an invitation email must register with Evidence.com. Users must have access to the email account that the administrator specified when adding the users to Evidence.com.

Invitations to join Evidence.com expire within 7 days. After an invitation expires, an agency administrator can re-invite the user.

**Note:** Agency administrators can assign devices to their agency’s Active users who have not yet registered on Evidence.com.

**1.** Locate the invitation email that Evidence.com sent to the address entered by your administrator while creating your Evidence.com user account.

---

**Dear Dave Shoe (Badge ID: SPD666),**

Spurbury PD has invited you to join Evidence.com, the secure digital management solution from Axon, with the Username: dshoe.

Please click the link below and follow the instructions to register and activate your account.

https://spurbury.qa.evidence.com/?id=UI%3Cpr=Register&token=C8490D614F60FBC644DD8DEF146053C6

**Important:** This invitation is only active for **7 days** and will expire on **03/22/2017 22:12:24**. To register after the link expires, you must ask your agency administrator to re-invite you.

If you are having problems with the registration link, please copy and paste the web address below into your web browser, click Register, and then enter your invite code:

https://spurbury.qa.evidence.com/?id=UI%3Cpr=Register&partner_id=8e6b12536f64ef3bd8295effb991c1e

Your invite code is: C8490D614F60FBC644DD8DEF146053C6

Sincerely,
The Axon Team
2. Click the first link in the email.
   
   Your default web browser opens your Evidence.com agency Registration page.

   **Note:** Alternately, in the email, copy the invite code and then click the second link. After the registration page opens, paste the invite code and click OK.

3. Complete the registration form.

4. Click **Submit**.
   
   Evidence.com sends you a welcome email.

### Re-Invite Users

Invitations to join Evidence.com expire within 7 days. After an invitation expires, an agency administrator can re-invite the user.

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.
   
   The All Users page lists all users in your agency. The row of buttons below the search filters includes a Reinvite Users button.

2. In the **Status** list, click **Active/Invited**, and then click **Search**.
   
   Evidence.com lists users whose status is Active but who have not yet completed user registration.

3. For each user you want to re-invite, select the check box next to the user name.

4. Click **Reinvite Users**.

5. On the confirmation message box, click **Yes**.
   
   Evidence.com sends the selected users a new invitation email.

### Deactivate Users

You can deactivate user accounts that have a status of Active. Evidence.com does not allow a user with a deactivated account to sign in.

When you deactivate a user account, the status of the user account is Inactive. Evidence.com sends the user an email stating that the account is deactivated.
You can deactivate users in two ways:

- Many users at once, from user-search results.
- One user at a time, from a User Summary page.

### Deactivate Many Users

From a user search page, you can deactivate more than one user account at a time.

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.

   The All Users page lists all users in your agency. The row of buttons below the search filters includes the Deactivate Users button.

2. In the **Status** list, click **Active**, and then click **Search**.

   Evidence.com lists users whose status is Active.

3. If you need to refine the search results more, use the search filters as needed.

4. For each user you want to deactivate, select the check box to the left of the user name. If you want to deactivate all users shown in search results, select the check box at the top left of the search results.

5. Click **Deactivate Users**.

   A dialog box for reassigning the users’ evidence and devices appears. By default, the “Evidence Files and Devices Remain Assigned to the Current User” option is selected.

6. If you do *not* want to reassign the users’ evidence and devices, skip to step 10.

7. If you want to reassign the users’ evidence and devices, click **Reassign the Evidence and Devices to Another User**.

8. In the **Reassign to** box, start typing the name of the user to whom you want to reassign evidence and devices. The user must belong to the same agency as the users whom you are deactivating.

   Evidence.com shows a list of users that match what you have typed.

9. Click the user to whom you want to reassign evidence and devices.

10. Click **Deactivate User**.

11. On the notification message box stating how many user accounts you deactivated, click **OK**.
Evidence.com sends a notification email to each user whose account you deactivated.

Because the User Results page does not automatically update, the user statuses continue to show as Active.

12. If you want to confirm that the accounts are deactivated, search for the users again.

**Deactivate One User**

From the User Summary page, you can deactivate a single user.

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.

   The All Users page lists all users in your agency.

2. Search for the active user whose account you want to deactivate.

3. In the user search results, click the user name.

   The User Summary page appears.

4. Click **Manage User**.

   The User Information page appears.

5. Click **Deactivate User**.

   A dialog box for reassigning the user’s evidence and devices appears. By default, the “Evidence Files and Devices Remain Assigned to the Current User” option is selected.

6. If you do not want to reassign the user’s evidence and devices, skip to step 10.

7. If you want to reassign the user’s evidence and devices, click **Reassign the Evidence and Devices to Another User**.

8. In the **Reassign to** box, start typing the name of the user to whom you want to reassign evidence and devices. The user must belong to the same agency as the user whom you are deactivating.

   Evidence.com shows a list of users that match what you have typed.

9. Click the user to whom you want to reassign evidence and devices.

10. Click **Deactivate User**.

11. On the notification message box states that the user account has been deactivated, click **OK**.
Account details for the deactivated user appear.

Evidence.com sends a notification email to the user whose account you deactivated.

### Reactivate Users

Agency administrators can reactivate previously deactivated users.

You can reactivate user accounts that have a status of Inactive.

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.

2. In the **Status** list, click **Deactivated**, and then click **Search**.

   Evidence.com lists users whose status is Inactive.

3. If you need to refine the search results more, use the search filters as needed.

4. For each user you want to reactivate, select the check box to the left of the user name. If you want to reactivate all users shown in search results, select the check box at the top left of the search results.

5. Click **Reactivate Users**.

   **Note:** You can reactivate a single user by clicking **Deactivated** under Status in the user’s row.

6. On the confirmation message box, click **OK**.

7. On the notification message box, click **OK**.

   Evidence.com sends each user an email stating that the user’s account active again.

   Because the User Results page does not automatically update, the user statuses continue to show as Deactivated.

8. If you want to confirm that the accounts are active, search for the users again.

### Unlock a User Account

When a user attempts and fails to sign in to Evidence.com more times than are allowed by the agency's security settings, the user is locked out of Evidence.com and receives the message, “Too many failed login attempts. Account temporarily suspended.”

You can unlock user accounts that are locked.
1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.

   The All Users page lists all users in your agency.

2. Search for the user whose account you want to unlock.

   User search results do **not** show whether an account is locked.

3. In the user search results, click the user name.

   The User Summary page appears.

4. Click **Manage User**.

   If the account is locked, the Unlock Account button is available.

5. Click **Unlock Account**.

6. On the confirmation message box, click **OK**.

   The user account is unlocked, the page refreshes, and the Unlock Account button is not available.

---

**Reset Passwords and Security Questions**

When you reset a user’s password and security questions, Evidence.com sends the user an email with information about the change and a temporary password that allows the user to sign in, change the password, and specify new security questions.

---

**Reset Password and Security Questions from a User Details Page**

You can reset the password and security questions of a single user from the User Details page.

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.

   The All Users page lists all users in your agency.

2. Search for the user whose password and security questions you want to reset.

3. In the user search results, click the user name.

   The User Summary page appears.

4. Click **Manage User**.

   The User Details page appears.
5. Click **Reset Credentials**.

6. On the confirmation message box, click **Continue**.

7. On the notification message box, click **OK**.

Evidence.com sends the user an email that explains that the user's password has been reset and provides instructions for creating a new password and security questions.

### Reset Passwords and Security Questions for Users from User Search Results

From the results of a user search, you can reset the password of more than one user accounts at a time.

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.

   The All Users page lists all users in your agency.

2. Search for users and refine the search until the search results includes users whose passwords and security questions you want to reset.

3. For each user whose password you want to reset, select the check box to the left of the user name. If you want to reset passwords for all users shown in search results, select the check box at the top left of the search results.

4. Click **Reset Password**.

5. On the confirmation message box, click **OK**.

6. On the notification message box, click **OK**.

   Evidence.com sends each user an email that explains that the user's password has been reset and provides instructions for creating a new password and security questions.

### Send a Message to a User

You can send a message to an active user.

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.

   The All Users page lists all users in your agency.

2. Search for the active user.

3. In the user search results, click the user name.
The User Summary page appears. The Send Message button is below the basic user information.

4. Click **Send Message**.

The Compose Message page appears.

5. In the **Subject** and **Message** boxes, type the subject and your message, and then click **Send**.

Evidence.com sends the message to the user you specified.

---

**Change a Username**

Administrators can change the username of a user account, if the user account status is Active.

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.

   The All Users page lists all users in your agency.

2. Search for the user whose username you want to change.

3. In the user search results, click the user name.

   The User Summary page appears.

4. Click **Manage User**.

5. Under **Account Details**, in the **Username** box, change the username, as needed.

6. Click **Save**.

   Evidence.com sends the user an email, notifying them of the change.

   All changes are tracked in the user audit trail.

---

**Edit Other User Account Information**

From the User Details page, administrators can update basic user information such as username, first name, last name, badge ID, email address, external ID, and user role.

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.

   The All Users page lists all users in your agency.
2. Search for the user whose details you want to edit.

3. In the user search results, click the user name.

   The User Summary page appears.

4. Click Manage User.

   The User Details page includes an Account Details area.

5. Update the Account Details section as needed and then click Save.

6. On the confirmation message box, click OK.

---

User Audit Trail

A user audit trail shows many of the activities taken by the user in addition to changes to the user account. User audit trails are available in two formats:

- PDF format — Well suited for use in court.
- Comma-separated values (CSV) format — Supported by spreadsheet applications such as Microsoft Excel and helpful for simplifying reporting and integration with other systems.

Evidence-related user actions that appear in user audit trails include the following:

- View evidence
- Watch video evidence
- Initiate evidence deletion
- Restore deleted evidence
- Upload evidence
- Add or edit evidence title
- Add or edit evidence ID
- Add or edit categories assigned to evidence
- Add or edit evidence location
- Edit evidence recorded date and time
- Flag or un-flag evidence
- Share evidence internally (with users in your Evidence.com agency)
- Share evidence externally (with users outside your Evidence.com agency)
- Add or edit evidence tags
- Add or edit evidence description
- Add, edit, or remove evidence notes
- Reassign evidence
- Add evidence to a case
- Add a marker
- Download a marker
- Add a video clip
- Add video redaction

Case-related user actions that appear in user audit trails include the following:

- Create case
- Viewed case
- Add evidence to a case
- Remove evidence from a case
- Share case by download link
- Share case with partner agency
- Share case with user in your agency (add member to case)
- Download case
- Add or remove folder
- Add or edit categories assigned to case
- Edit case title
- Add or edit case description
- Add, edit, or delete case notes
- Add or remove case tags
**Get a User Audit Trail**

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.
2. Search for the user whose audit trail you want to view.
3. In the user search results, click the user name.
   
   The User Summary page appears.
4. Click **View Audit Trail**.
   
   A dialog box provides options for the date range and file type.
5. Under **Select Date Range**, do one of the following:
   - If you want to view the whole audit trail, select **View entire audit trail**.
   - If you want to view a portion of the audit trail, select **View portion of audit trail**, either specify a date in either or both the **From** or **To** boxes or click a shortcut for a date range, such as Yesterday.
6. Under **Select File Type**, click the file type that you want.
   
   Evidence.com downloads the user audit trail in the format you selected.
7. Save or view the audit trail file, as needed.

**Expire All Passwords**

An administrator can force agency-wide password resets.

1. On the menu bar, click **Admin** and then under **Security Settings**, click **Password Configuration**.
2. Under **Force Password Expiration for All Users**, click **Expire All Passwords**.
3. On the confirmation dialog box, click **Continue**.
   
   The next time each user signs in to your agency, Evidence.com requires that they change passwords.
Groups Administration

The Groups feature can be used to leverage the access control workflow to grant access to group members. This can reduce the number of individual users that have to be added to or removed from an evidence Access List. Additionally, if individual group members are added to or removed from the Group, those individuals will gain or lose access to existing Group evidence without having to take any other action.

Groups can also provide additional control of what evidence can be viewed by users. For example, with groups, you can grant unit leaders the ability to view the evidence of their team members only.

The Groups feature complements the Roles and Permissions feature. Unit leaders no longer must be granted permission to view all evidence of your agency, and you should remove this permission from leaders when you implement the Groups feature.

This section describes the Groups feature, the use of groups for evidence monitoring, and the group-related tasks that you can perform.

Groups and Membership

Each group that you create has a name, one or more members, and an access setting. Group members can be users, groups, or a mix of users and groups. Users and groups can be members of more than one group. There are no default groups.

The following figure shows two groups that each have three users. The user in the middle is a member of both groups.
The following figure shows two groups that each have three users. Group 2 is made up of one user, that is shared with group 1, and another group.

Managing Group Access

You can set group access so it is able to be added evidence access list inside your agency and to be added to access lists at partner agencies.

There are three Manage Access Settings for a Group:

- **No access**: The Group cannot be added to any access lists.
- **Inside my agency access**: The Group can be added to evidence access lists inside your agency, but partner agencies will not see the Group in their access lists.
- **Partner agency access**: The Group can be added to access lists inside your agency and at partner agencies.

When a partner agency grants access to evidence, they can add any groups that have partner agency access. All members and monitors of the group receive a message notifying them that they have been granted access to the evidence.

For more information, see the Receiving Shared Cases from Partner Agencies section.

A group that is monitoring a group that receives a shared case from a partner agency can view the evidence of the shared case.
Monitoring Evidence with Groups

You can use the Groups feature to control whose evidence a user can view. For each group, you can specify users and other groups that can view the evidence owned by group members.

In order to take advantage of this capability, your group organization strategy should include:

- Groups of users whose evidence needs to be monitored, such as unit members.
- Groups of users who need to monitor evidence, such as unit leaders.

In the following figure, the group 3, 4, and 5 monitors are granted access to evidence owned by users in their respective groups. Additionally, users in group 1 are granted access to evidence owned by users in groups 3 and 4, but not group 5.

![Diagram showing evidence access](image)

**Note:** In the preceding example, users who do not monitor group 5 evidence but who are allowed the User Search permission can see group 5 evidence listed in evidence search results but cannot view the evidence without first requesting access.

For users who must both monitor evidence and have their evidence monitored, add the users to groups being monitored and to groups who are monitoring. For example, in the preceding figure, users who are members of groups 1 and 3 can:

- Monitor the evidence of users in groups 3 and 4
- Have their evidence monitored by other users in group 1.
More than one group can monitor the evidence of another group. In the following figure, groups 1 and 2 have permission to monitor the evidence of group 4.

Group States

A group can be in one of two states:

- **Active** — From the moment you create a group and until you delete it, its state is Active. All group-related features are available for active groups.

- **Deleted** — When you no longer need a group, you can change its state to Deleted. The only feature available for a deleted group is the ability to view the audit trail of the group.

Permissions and Groups

To benefit from the Groups feature, you should review the assignment of a key permission: whether users are permitted to view all evidence or only their own.

When you implement group-based evidence monitoring, users need the permission to view their own evidence only. When you add a user to a monitoring group, the Groups feature enables the user to view the evidence of all members in the groups being monitored.

If you previously allowed leaders to view all evidence in order to enable them to view the evidence of their subordinates, when you implement the Groups feature, you should change the permissions of leaders to view their own evidence only and rely on the Groups feature to enable appropriate access to evidence.
Additionally, the Groups feature has no effect on whether evidence search results show a user evidence that the user does not have permission to view. If a user is allowed the User Search permission, evidence search results list evidence that the user does not have permission to view, but from search results, the user can request access to the evidence.

Evidence.com also provides permissions for the following actions:

- Creating, updating, and deleting groups.
- Viewing group audit trails.

## Implementing Groups

The following steps provide a guideline for implementing the Groups feature at your agency. Where additional detail is available in other locations in this guide, cross-references are provided.

1. Decide upon a strategy for using the Groups feature. Your agency can determine the best way to use groups for controlling access to evidence and for monitoring the evidence-related activities of group members.

   If your agency needs to keep its Evidence.com group configurations in sync with groups in other applications, such as with an on-premises Microsoft Active Directory implementation, review the information in Import Groups, Members, and Monitors.

2. Update roles and permissions as needed to ensure that users have only the permissions that their responsibilities require.

   - Users who are enabled by the Groups feature to monitor evidence should be allowed the Only Their Own setting for the Evidence View permission.
   - Users whose evidence search results should not list evidence that they do not have permission to view should be prohibited the User Search permission.
   - Users who create, update, and delete groups must be allowed the Create/Edit Group permission.
   - Users who import groups, members, and monitors must be allowed the Configure Agency Security Settings permission.
   - Users who view group audit trails must be allowed the Group Audit Trail PDF permission.

   For detailed steps, see Update Roles and Permissions.
3. Following your group strategy, create groups and assign members and monitors to the groups.
   - For information about creating many groups, see Import Groups, Members, and Monitors.
   - For information about creating one group at a time, see Create a Group.

4. Use the Group Profile page to view evidence uploaded by group members. For detailed steps, see View All Evidence.

5. As needed, add and remove users from groups or update other group settings. For detailed steps, see Edit Group Members, Monitors, and Other Settings.

6. As needed, view the audit trail of groups. For detailed steps, see View Group Audit Trail.

7. When a group is no longer needed, delete the group. For detailed steps, see Delete Group.

8. Continue creating, using, managing, and deleting groups as needed.

---

**Update Roles and Permissions**

Administrators or users with permission to edit agency settings can update roles and permissions so that your agency can use the Groups feature to control access to evidence.

**User Permissions**

Users who monitor the evidence of other users need permission to view only their own evidence. On the Configure Role page, under Evidence Management, the View permission includes the “Only Their Own” option.

**Note:** If License Tiers are enforced or in preview mode for your agency, Group Monitors must be assigned to a Pro Tier role.

Users whose evidence search results should not list evidence that they do not have permission to view should be prohibited the User Search permission. On the Configure Role page, under Search Access, the User Search permission includes the Prohibited option.

When you implement the Groups feature, you can rely on the ability of monitoring groups to view the evidence uploaded by members of the groups that they monitor.

For more information about editing permissions in a role, see Edit a Role.
Group Management and Audit Permissions

Users whose responsibilities include creating, updating, and deleting groups must be allowed permission to create and edit groups. On the Configure Role page, under User Account, the Create/Edit Group permission includes the Allowed option.

Users whose responsibilities include importing groups, members, and monitors must be allowed permission to change agency security settings. On the Configure Role page, under Admin Access, the Configure Agency Security Settings permission includes the Allowed option.

Users whose responsibilities include viewing group audit trails must be allowed permission to view the audit trails. On the Configure Role page, under User Account, the Group Audit Trail PDF permission includes the Allowed option.

For more information about editing permissions in a role, see Edit a Role.

Create a Group

Users with permission to create a group can do so as needed.

At a minimum, when you create a group, you specify the group title. You can also add users and other groups as members, specify evidence-monitoring permissions, and specify whether the group can receive shared evidence from partner agencies.

1. On the menu bar, click Admin and then under Users, click Create Group. The Create Group page appears.
2. Name the Group and set the Manage Access Setting

The group title must be at least three characters long and can be a maximum of 128 characters long.

There are three Manage Access Settings for a Group:

- **No access**: The Group cannot be added to any access lists.
- **Inside my agency access**: The Group can be added to evidence access lists inside your agency, but partner agencies will not see the Group in their access lists.
- **Partner agency access**: The Group can be added to access lists inside your agency and at partner agencies.

Note that for any Manage Access Setting, Group Monitors can view evidence owned by Group Members.

3. Click **Create**.

4. For each user or group that you want to add as a group member, in the **Add Members** box, start typing the name of the user or group, wait for Evidence.com to show the list of matching users or groups, click the user or group that you want, and then click **Add**.

When all group members have been added, click **Next**.

5. **Add Monitoring Relationships** (optional). The final step when creating a group is adding monitoring relationships for the group. A Group’s monitoring relationship is independent of the Group’s Manage Access Settings.
Note: If License Tiers are enforced or in preview mode for your agency, Group Monitors must be assigned to a Pro Tier role.

There are two types of monitoring relationships:

- **Monitors of this Group:** This sets the users and groups that can access evidence owned by members of this group.

- **This Group can Monitor:** This allows group members to access evidence owned by members of the specified groups. In other words, you are effectively assigning all Group Members as Monitors of the specified Groups.

If you do not want to add any monitoring relationships, go to step 6.

Otherwise, once you have decided which type of Monitoring Relationship to use, click the appropriate text box and start typing the name of the user or group, wait for Evidence.com to show the list of matching users or groups, click the user or group that you want, and then click **Add**.

6. When all monitoring relationships have been added, click **Done**.

The Group Profile page shows the members and monitors of the group.
Import Groups, Members, and Monitors

Administrators and users allowed the Configure Agency Security Settings permission have a swift and scalable way to manage Evidence.com groups. The Import Groups feature lets you use comma-separated value (CSV) files to create groups and to define group members and monitors. The Import Groups feature is available on the Admin Portal page.

Import Groups provides separate processes for defining groups and for configuring group members and monitors. A different CSV file is required for each process. For more information about the CSV files, see Import Groups and Define Members and Monitors.

Strategies for Importing Groups, Members, and Monitors

It is recommended that you consider how your organization can best make use of the Import Groups feature.

Setup by Import, Maintain by Import

The primary use for the Import Groups feature is to enable agencies to keep their Evidence.com group configurations in sync with groups in other applications, such as with an on-premises Microsoft Active Directory implementation.

With this strategy, it is recommended that your groups CSV file and members-and-monitors CSV file reflect the complete configuration of all groups and their members and monitors. It is also recommended that you ensure that the CSV files are backed up reliably.

Setup by Import, Maintain Manually

If you have no need to synchronize group configuration with an external source, consider using the Import Groups feature when you are setting up groups for the first time. Rather than creating groups one at a time, you can define the groups and their members and monitors using CSV files, and then import the files.

After importing groups and defining members and monitors, you can review your group configuration in Evidence.com and update it as needed. If a large number of changes are needed, it is likely more efficient to update the CSV files and reimport them.

When you are satisfied with your initial group configuration, you can begin maintaining groups individually, as described in Edit Group Members, Monitors, and Other Settings.
Empty Groups

You cannot use the Define Members and Monitors feature to empty an existing group of all members and monitors. It is recommended that you delete a group rather than trying to maintain an empty group. You can always create the group again later, when it is needed.

Import Groups

The CSV file for importing groups must contain a header row and must have three columns. A sample ImportGroups.csv file is available on the Import Groups page. The following table describes the required values in the CSV file for importing groups:

<table>
<thead>
<tr>
<th>Column</th>
<th>Header Value</th>
<th>Value</th>
</tr>
</thead>
</table>
| A      | EXTERNAL_ID     | External group ID — A unique value that identifies the group. This ID should be persistent and unchanging for the life of the group. The ID is assigned by your organization. It is recommended that you determine a group ID strategy that best suits your needs.  
If you are manually synchronizing the groups in your Evidence.com agency with groups in another application, you may want to use an ID value provided by the other application, such as a GUID.  
To find the external group ID for an existing group, view the Group Profile page for the group.  
You can also simply assign a descriptive name.  
Valid external group IDs can be up to 255 characters. |
| B      | NAME            | Group title — A meaningful name for the group. Because EXTERNAL_ID value provides the persistent identifier for the group, you can change the NAME value as needed.  
Valid group titles can be up to 128 characters. | |
| C      | SHARE_ACCESS    | Sets the access levels for the group and corresponds to the Manage Access Settings. Valid values are the following three words:  
• FORBIDDEN: The Group cannot be added to any access lists. This corresponds to the No access setting.  
• INTERNAL: The Group can be added to evidence access lists inside your agency, but partner agencies will not see the Group in their access lists. This corresponds to the Inside my agency access setting.  
• ANY: The Group can be added to access lists inside your agency, and partner agencies will see and can add the Group in their access lists. This corresponds to the Partner agency access setting. |

Note: Older versions of the Import Groups csv with the VISIBLE_TO_FEDERATED column will be accepted for upload, but the values imported will be converted to the new SHARE_ACCESS setting as follows:
VISIBLE_TO_FEDERATED = TRUE is converted to SHARE_ACCESS = ANY
VISIBLE_TO_FEDERATED = FALSE is converted to SHARE_ACCESS = FORBIDDEN

For more information about valid CSV formatting, see https://tools.ietf.org/html/rfc4180

1. If you have already prepared your groups CSV file, skip to step 9.
2. On the menu bar, click Admin and then, under Users, click Import Groups.
3. Under Import Groups, click ImportGroups.csv and save it to your computer.
4. Make a copy of the ImportGroups.csv file and assign it a meaningful file name.
   This new file is your groups CSV file.
5. Open the file in a spreadsheet application, such as Microsoft Excel.
6. Delete the second, third, and fourth rows. Do not delete the first row. Evidence.com expects the first row to contain the column names.
7. For every group that you want to add, include a row in the file that specifies values for the group, as described in the preceding table. Ensure that each value is in the cell beneath the applicable header.
8. Save your groups CSV file.
9. In Evidence.com, if your session has timed out, sign in again and return to the Import Groups page by clicking Admin and then, under Users, clicking Import Groups.
10. If you want to completely replace all groups currently in your agency with the groups in your groups CSV file, click to clear the Do Not Make Changes To Any Groups That Currently Exist check box.
Note: It is recommended that you use the Do Not Make Changes To Any Groups That Currently Exist check box with caution. If you clear the check box and import a CSV file, only the groups in the CSV file exist after the import. Any other groups that previously existed in your agency are deleted.

11. If you want to add the groups in the CSV file without affecting any existing groups, select the Do Not Make Changes To Any Groups That Currently Exist check box. By default, the Do Not Make Changes To Any Groups That Currently Exist check box is selected.

12. Next to Groups File, click Choose File and, in the dialog box that opens, select the groups CSV file on your computer, and then click Next.

Evidence.com displays a list actions taken based on the groups found in the uploaded file. This includes information about errors that Evidence.com detected and about the deletion of previously existing groups that were not defined in the groups CSV file.

13. Review the list of actions taken.

14. If you need to correct errors, update the groups CSV file as needed, click Import More Groups, Members, and Monitors, and repeat this procedure.

15. Click Finished.

The All Groups page appears.

Define Members and Monitors

You can import definitions for group members and monitors. You define the members and monitors in a CSV file.

Note: If License Tiers are enforced or in preview mode for your agency, Group Monitors must be assigned to a Pro Tier role.

Each row in the members-and-monitors CSV file defines a single member or monitor for a single group. For example, if you wanted to add a user as both a member and a monitor to a group, the CSV file would include two rows: one row for adding the user as a member and a second row for adding the user as a monitor.

Note: Only the groups referenced in column A of the members-and-monitors CSV file are affected when you define members and monitors. For example, if groups 1 and 2 each have several members assigned and then you import a members-and-monitors CSV file that only includes rows that define members and monitors for group 1, Evidence.com takes no action on group 2.
The members-and-monitors CSV file must contain a header row and must have four columns. A sample ImportMembersAndMonitors.csv file is available on the Import Groups page. The following table describes the required values in the CSV file for defining members and monitors:

<table>
<thead>
<tr>
<th>Column</th>
<th>Header Value</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>EXTERNAL_ID</td>
<td>External group ID — The ID of the group to which the member or monitor is added. This ID must match the external group ID used to create the group. For more information, see Import Groups. If you specify an external group ID that does not correspond to an existing group in your agency, Evidence.com does not create the member or monitor and an error message appears in the list of actions taken. Valid external group IDs can be up to 255 characters.</td>
</tr>
<tr>
<td>B</td>
<td>MEMBERSHIP_TYPE</td>
<td>Member or monitor — Whether the row in the CSV file defines a member or a monitor. Valid values are the following two words: MEMBER, MONITOR The valid values are case insensitive.</td>
</tr>
<tr>
<td>C</td>
<td>ENTITY_TYPE</td>
<td>User or group — Whether the member or monitor is a user or a group. Valid values are the following two words: USER, GROUP The valid values are case insensitive.</td>
</tr>
<tr>
<td>D</td>
<td>ENTITY_ID</td>
<td>Identifier of the member or monitor. If the member or monitor is a group, this value is the external group ID, which must match the external group ID used to create the group. If the member or monitor is a user, this value must be the email address configured in the user account in your Evidence.com agency.</td>
</tr>
</tbody>
</table>

For more information about valid CSV formatting, see https://tools.ietf.org/html/rfc4180

1. If you have already prepared your members-and-monitors CSV file, skip to step 9.
2. On the menu bar, click Admin and then, under Users, click Import Groups.
3. Under **Define Members and Monitors**, click **ImportMembersAndMonitors.csv** and save it to your computer.

![Define Members and Monitors](image)

4. Make a copy of the **ImportMembersAndMonitors.csv** file and assign it a meaningful file name.

   The new file is your members-and-monitors CSV file.

5. Open the file in a spreadsheet application, such as Microsoft Excel.

   ![Spreadsheet](image)

6. Delete the second, third, fourth, and fifth rows. **Do not** delete the first row. Evidence.com expects the first row to contain the column names.

7. For every member or monitor that you want to add to a group, include a row in the CSV file that specifies values for the member or monitor, as described in the preceding table. Ensure that each value is in the cell beneath the applicable header.

8. Save the file.

9. In Evidence.com, if your session has timed out, sign in again and return to the Import Groups page by clicking **Admin** and then, under **Users**, clicking **Import Groups**.

10. If you want to **completely replace all members and monitors** in the groups referenced in column A of the members-and-monitors CSV file, click to clear the **Do Not Remove Group Members Or Monitors That Currently Exist** check box.

    **Note:** It is recommended that you use the Do Not Remove Group Members Or Monitors That Currently Exist check box with caution. If you clear the check box and import a CSV file, then in the groups referenced in column A of the CSV file, only the members and monitors defined in the CSV file exist after the import. Any other members and monitors that previously existed those groups are removed. Groups not referenced in column A of the CSV file are unaffected.
11. If you want to add the members and monitors in the CSV file without affecting any existing members and monitors, select the **Do Not Remove Group Members Or Monitors That Currently Exist** check box.

By default, the Do Not Remove Group Members Or Monitors That Currently Exist check box is selected.

12. Next to **Members and Monitors File**, click **Choose File** and, in the dialog box that opens, select the CSV file on your computer, and then click **Next**.

Evidence.com displays a list actions taken based on the members and monitors found in the uploaded file. This includes information about errors that Evidence.com detected.

13. Review the list of actions taken.

14. If you need to correct errors, update the CSV file as needed, click **Import More Groups, Members, and Monitors**, and repeat this procedure.

15. Click **Finished**.

The All Groups page appears.

---

**Search and View Groups**

As with the management of evidence, cases, devices, and users, Evidence.com provides a search feature to help you find groups that you need to work with.

For each group in search results, you can access a Group Profile page, which shows the group title and number of members. The external ID appears below the group title. For groups created by the Create Group page in Evidence.com, the external ID is a hyphenated hexadecimal number automatically assigned by Evidence.com. For groups created by an external source, such as imported CSV file, the Evidence.com Partner API, or automatic provisioning with Microsoft Azure Active Directory, the external ID is the value assigned by external source.
The page also provides access to the group monitor list, the group audit trail, a list of all evidence owned by members of the group, and whether the group can receive evidence shared by a partner agency.

Users with permission to perform user searches can access the Group Search feature on the Users menu.

1. On the menu bar, click **Admin** and then under **Users**, click **All Groups**.

   The All Groups page shows the search filters and the default search results.

2. If you want more specific results, set the group search options and click **Search**.

   **Note:** The Member and Monitor search options support filtering by users only. You cannot filter by groups who are members or monitors.

   The search results appear below the search form. Deleted groups appear in search results so that you can access their audit trails.

3. If you want to sort the results, click the column that you want to sort by. You can sort by group title, status, date last modified, and whether groups can receive cases shared by partner agencies.

4. If you want to improve the search results, update the search options as needed, and click **Search** again.

5. If you want to view details about a group, click the group title.

   The Group Profile page appears.

---

**Dashboard List for Monitors**

If a user is a monitor of one or more groups, the Groups I Monitor section appears on the user's Dashboard. This area lists the groups in which the user is a monitor. For each group in the list is link to the applicable Group Profile page. For more information, see Dashboard.
My Profile Page for Members and Monitors

A user’s account profile page may include group-related lists.

- Groups I Monitor — Appears if the user has evidence-monitoring permission for a group.
- Groups I Am Member Of — Appears if the user is a member of any group.

The user can access the profile page for a group by clicking the group title.

For more information about the user account page, see Update Your Basic Account Information.

User Accounts of Members and Monitors

Administrators and others who are allowed the User Administration permission can see a “Groups I Monitor” list on the profile page of any user who has evidence-monitoring permission for a group. For more information about accessing a user profile page, see Edit Other User Account Information.

Edit Group Members, Monitors, and Other Settings

Users with permission to edit a group can make changes to all settings associated with a group.

Note: If License Tiers are enforced or in preview mode for your agency, Group Monitors must be assigned to a Pro Tier role.

1. In your Evidence.com agency, search for the group for which you need to make changes.
2. In the group search results, click the group title.
   The profile page for the group that you clicked appears.
3. Edit the group as needed. For detailed steps, refer to the following table.

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the group name</td>
<td>1. To the right of the group name, click (edit).</td>
</tr>
<tr>
<td></td>
<td>2. Type the new name.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>
### Task | Steps
--- | ---
**Add a user or group to any of the following:**
- Members
- Monitors of this group
- Who this group can monitor
1. As needed, click to expand the panel you need to open – **Members** or **Monitors**.
2. Click in the box that you need: **Add Member**, **Monitors of this Group**, or **This Group Can Monitor**.
3. Start typing the name of the user.
4. Wait for Evidence.com to show the list of matching users.
5. Click the user you want to add.
6. Click **Add**.

**Delete a user or group from any of the following lists:**
- Members
- Monitors of this group
- Who this group can monitor
1. As needed, click to expand the panel you need to open – **Members** or **Monitors**.
2. In the list that you need to edit, find the user or group.
3. To the left of the user or group name, under **Actions**, click **X**.

**Change the group Manage Access Setting**
1. To the right of Access Settings, click **(edit)**.
2. Select the appropriate Manage Access Setting for the group.
3. Click **Save**.

**Copy the external ID of the group**
The external ID appears below the group title. To copy it, click the icon to the right of the external ID.

### View All Evidence

Users who have evidence-monitoring permission for a group can view a list of all the evidence uploaded by group members or shared with the group by a partner agency. Administrators can also view all evidence owned by group members.

1. In your Evidence.com agency, search for the group for which you need to view evidence. For more information, see Search and View Groups.

2. In the group search results, click the group title.
   
   The Group Profile page appears.

3. Click **View All Evidence**.
   
   The All Evidence page lists all evidence uploaded by members of the group or shared with the group by a partner agency.

4. If you want to view evidence, click the evidence title.
   
   Evidence.com displays detailed information about the evidence.
5. If you want access to another member’s evidence, click Request Access for the evidence.

Evidence.com sends you a notification email when the member has granted you access to the evidence.

---

**View Group Audit Trail**

Users who have permission to view group audit trails can do so from the Group Profile page of any group. For deleted groups, viewing the audit trail is the only available action.

To perform this task, you must be allowed the Group Audit Trail PDF permission.

1. In your Evidence.com agency, search for the group for which you need to view the audit trail. For more information, see Search and View Groups.

2. In the group search results, click the group title.

   The Group Profile page appears.

3. Click **View Audit Trail**.

   A dialog box provides options for viewing the entire audit trail or a portion of the audit trail.

4. If you want to view the whole audit trail, under **View entire audit trail**, click **Submit**.

5. If you want to view a portion of the audit trail, under **View portion of audit trail**, specify a date in either or both the **From** or **To** boxes and click **Submit**.

   Evidence.com opens or downloads a PDF for the agency audit trail. The exact behavior depends on the browser you use and its download settings for PDF files.

6. Save or view the audit trail PDF as needed.

---

**Delete Group**

Users who have permission to edit groups can change the status of an active group to Deleted. When you delete a group, the access of monitors to evidence uploaded by members of the group is revoked.

**Note:** Deleted groups cannot be re-activated.

The audit trail for a deleted group remains available for users who have permission to view group audit trails.
**Delete Group from Group Search Results**

1. In your Evidence.com agency, search for the group you want to delete.

2. In the group search results, to the left of the group title, click \( \text{delete} \) (delete).

3. On the confirmation message box, click **Delete**.

   Evidence.com changes the state of the group to Deleted.

   If the group search results include only groups that are Active, Evidence.com removes from the results the group that you deleted.

**Delete Group from Group Profile Page**

1. In your Evidence.com agency, search for the group you want to delete.

2. In the group search results, click the group title.

   The Group Profile page appears.

3. Click **Delete Group**.

4. On the confirmation message box, click **OK**.

   Evidence.com changes the state of the group to Deleted.

   The Edit Group Profile page updates and the only action available is View Audit Trail.

---

**Roles and Permissions**

Roles determine user permissions, which control access to features and functions. Each Evidence.com user is assigned a role.

Administrators and users whose role has the Edit Agency Settings permission set to Allowed can create and edit roles. Administrators and users whose role has the User Administration permission set to Allowed can assign roles to users.

By default, Evidence.com provides all agencies with pre-configured roles and locked roles. Locked roles cannot be changed by your agency.

<table>
<thead>
<tr>
<th>Pre-Configured Role</th>
<th>Locked or Configurable</th>
<th>Required License Tier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>Locked</td>
<td>Pro</td>
</tr>
</tbody>
</table>

Axon Enterprise, Inc.

Page 248 of 344
### Pre-Configured Role

<table>
<thead>
<tr>
<th>Role</th>
<th>Locked or Configurable</th>
<th>Required License Tier</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Configurable</td>
<td>Basic (Pro if a Pro license permission is allowed)</td>
</tr>
<tr>
<td>Investigator</td>
<td>Configurable</td>
<td>Pro</td>
</tr>
<tr>
<td>Armorer</td>
<td>Configurable</td>
<td>Basic (Pro if a Pro license permission is allowed)</td>
</tr>
<tr>
<td>Lite User</td>
<td>Locked</td>
<td>N/A</td>
</tr>
<tr>
<td>Lite Armorer</td>
<td>Locked</td>
<td>N/A</td>
</tr>
</tbody>
</table>

The Lite User and Lite Armorer roles are designed for users that only work with TASER Conducted Electrical Weapons (CEW) logs and TASER CAM videos. The Lite Armorer role acts as a CEW administrator and can reassign agency CEW devices, change CEW settings, and upload any CEW logs.

For more information about the permissions associated with each pre-configured role, see the [Pre-Configured Roles](#) section of Appendix A.

### About the Access Restricted Evidence Permission

In general, if evidence has been assigned to a [Restricted Evidence Category](#), then access to the restricted evidence is controlled by the access list. But users can also be assigned to roles with the Access Restricted Evidence permission, which allows the users to access to all restricted evidence in your agency.

This permission is in the Evidence Management permissions section and requires a Pro License.

### Dependencies Among Permissions

Some permissions are not configurable unless one or more related permissions that they are based upon are allowed. Additionally, some permissions require a Pro license to be configured.

For example, when creating or editing a role, the Evidence Management - Edit permission is not available unless the Evidence Management - View permission is not set to Prohibited. Similarly, the Evidence Management - Redact permission is not available unless Evidence Management - Edit permission is not set to Prohibited and the Role Tier is set to Pro.

Evidence.com provides descriptions of each permission, including their dependencies, on the Configure Role page. You can also refer to [Appendix A: Roles and Permissions](#), in this guide for this information.
Planning Roles

1. Review the pre-configured roles and the permissions.
   For more information, see Appendix A: Roles and Permissions.

2. Assess the permission-related needs of your organization. For example, consider which users need to:
   - View evidence owned by other users
   - Create cases and share cases with others in your agency
   - Share cases with your partner agencies
   - Generate reports
   - Administer your agency's security settings
   
   Note: It is recommended to allow access to ‘Any evidence’ only for administrative or investigatory roles

3. Design a role strategy that meets your organization’s needs and number of Evidence.com Pro and Basic licenses.
   In order for the administration of your Evidence.com agency to remain manageable, it is recommended that you keep your role strategy as simple as you can while meeting your organization's needs.

4. As needed, add and edit roles to implement your role strategy.

5. Assign users to the appropriate roles.

Add a Role

Administrators and users whose role allows the Edit Agency Settings permission can create roles that suit the security needs of your agency.

1. On the menu bar, click Admin and then under Agency Settings, click Roles & Permissions.
   The Roles & Permissions page lists available roles in alphabetical order.

2. Click Create Role.
   The Configure New Role page appears.
3. **In the Role Name box**, type a name for the role.

   By default, all permissions are prohibited, except for the permissions under Login Access.

   **Note:** To view a description of a permission, click the name of the permission.

4. **Select the license Tier associated with the role.**

5. For each permission that you need to update, locate the name of the permission on the page, and then to the right of the name, click the option you need.

6. **When you have finished setting permissions**, scroll to the bottom of the page and then click **Save**.

   The Roles & Permissions includes the new role in the alphabetical list of roles.

---

**Edit a Role**

Administrators and users whose role allows the Edit Agency Settings permission can make changes to custom roles and to unlocked, pre-configured roles.

If you edit a role to change any of the Login Access permissions, all users assigned to the role receive a notification email about the change.

1. **On the menu bar**, click **Admin** and then under **Agency Settings**, click **Roles & Permissions**.

   The Roles & Permissions page lists available roles in alphabetical order.

2. **Click the **edit** icon on the same line as the role that you want to edit.**

   The Configure Role page lists the permissions and their settings for the role.

3. **If you want to rename the role**, in the **Role Name** box, type the new name.

4. **If you want to change the license tier associated with the role**, select the new license **Tier**.

5. **For each permission that you need to update**, locate the name of the permission on the page, and then to the right of the name, click the option you need.

   You may need to scroll the page until the permission is visible.

   **Note:** To view a description of a permission, click the heading name for the group associated with the permission.
6. When you have finished editing the role, scroll to the bottom of the page and then click **Save**.

Evidence.com immediately begins enforcing the changes to permissions that you made.

---

**Copy a Role**

You can copy the permission settings from an existing role to a new role using the duplicate function.

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Roles & Permissions**.

   The Roles & Permissions page lists available roles in alphabetical order.

2. Click the 🔄 icon on the same line as the role that you want to copy.

   The Configure Role page lists the permissions and their settings for the role.

3. Scroll to the bottom of the page and click **Duplicate**.

4. Enter a name for the new role and click **OK**.

5. If you want to change the license tier associated with the role, select the new license **Tier**.

6. If you want to change a permission setting, locate the name of the permission on the page and then click the option you need.

   You may need to scroll the page until the permission is visible.

   **Note:** To view a description of a permission, click the heading name for the group associated with the permission.

7. When you have finished editing the role, scroll to the bottom of the page and then click **Save**.

---

**Assign a Role to Users**

Agency administrators can assign a role to users by using the Roles & Permissions page.

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Roles & Permissions**.

2. Click **Assign Roles**.
The All Users page lists all users in your agency.

3. Search for users and refine the search until the search results includes the users to whom you want to assign a role.

4. For each user to whom you want to assign a role, select the check box to the left of the user name, and then click **Update Role**.

   The Assign Role dialog box appears.

5. In the **Role** list, click the role you want to assign to the selected users, and then click **OK**.

   **Note:** The license tier associated with each role is shown next to the role name in parenthesis.

6. On the confirmation message box, click **OK**.

   In the search results, the newly applied user roles appear.

---

**Citizen Settings**

Agency Evidence.com administrators should set up the agency Axon Citizen settings as needed for your Axon Citizen implementation before allowing users to send individual invitations.

Before allowing users to create portals or invitations, select the Axon Citizen settings for contact information requirement. An agency can choose to require contact information to be stored in Evidence.com and the select the required fields when information is stored. The settings for required fields apply anytime an invitation is sent with the contact information to be stored in Evidence.com.

---

**Configure Citizen Settings**

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Citizen Setting**.

   The Citizen Settings page is shown.
2. Set the **Retention Period for Declined Submission** options.

   This setting applies for both individual invites and public portals.

   If evidence that is declined during triage should have a custom retention date, toggle **Use Custom Retention Period** to on (blue = on). Select the **Retention Period** interval (Days, Weeks, Years) and enter the Retention Period length.

3. In the Invitation Invite Settings section, select if the ID and Category fields are required, optional, or not shown to senders for individual invitations.
• If **Required** is selected, the evidence collector must enter the information before an individual invitation is sent.

• If **Do Not Show** is selected, the field is not shown to the evidence collector.

4. In the Community Member Info section, select if your agency will **Require contact information to be stored in Evidence.com** for individual invites.

   Selecting this setting removes the Store Contact Information option for evidence collectors when creating individual invitations and the contact phone number or email will be stored in Evidence.com.

   • If required, select the information fields that are required whenever contact information is stored in Evidence.com for individual invites.

5. Select the **Auto-Accept Submissions** setting for individual invites (blue = on).

   When on, submissions from individual invites are automatically accepted and placed in active status. Otherwise, users must manually accept or decline each evidence submission.

6. In the Public Portals Settings section, select if your agency will **Require contact information to be stored in Evidence.com** for portals.

   • If required, select the information fields that are required whenever contact information is stored in Evidence.com.

7. Click **Save Settings**.

   The Citizen Settings are saved.

---

**Transcription Service**

The Evidence.com on-demand transcription service allows you to order transcriptions of any video or audio stored in Evidence.com, such as body camera video, in-car video, interview-room video and audio, and Axon Capture recordings.

After transcripts are completed, they are automatically stored in Evidence.com as accompanying metadata for easy access and sharing, without jeopardizing the chain of custody.

Transcriptions are rendered by a Criminal Justice Information Services (CJIS)-compliant provider on a pay-as-you-go basis using US-based transcriptionists. Transcriptions are normally completed within 24 hours of the request.
Agencies that allow officers to verbally summarize report information in a recording or to a secretary to be typed out can use the transcription service for this purpose by having the officer record and upload the report to Evidence.com.

The Evidence.com on-demand transcription service currently integrates with SpeakWrite for transcriptions. For more information about SpeakWrite, please visit: www.speakwrite.com/axon.

We will announce partnerships with other law-enforcement transcription providers as they become available.

**Note:** This service is currently only available for customers in the United States, but will be expanding to other regions in the future.

### Transcription Service Setup

Before the Evidence.com on-demand transcription service can be used, the service must be set up with the transaction provider. Additionally, the Order Transcript permission must be enabled in Evidence.com for the appropriate Roles.

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Transcription Settings**.

   **Note:** If you already have a SpeakWrite ID, click the **Click here** link under Begin Setup and skip to step 6.

2. Click **Begin Setup**.

   This opens the SpreakWrite for Axon Evidence.com website a new browser tab or window.
3. Click **Sign Up**.

4. Enter your information in the SpeakWrite system and then click **Create an Account**.
5. Copy your SpeakWrite ID.

You are directed back to the SpeakWrite website. SpeakWrite will contact your agency to complete the setup.

After your setup is complete, enable the Order Transcript permission for the appropriate Roles in Evidence.com.
**Agency Profile**

The agency profile enables you to specify details about your agency, such as street address, logo, and description. Through the Agency Profile page, you can access the agency audit trail.

### Configure Agency Street Address

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Agency Profile**.
   
   The Agency Profile page appears.

2. Click **Edit Address**.

3. In the boxes and lists provided, specify the agency street address.

4. When you have finished editing the address, click **Submit**.

5. On the notification message box, click **OK**.

   The Agency Profile page displays the new street address.

### Configure Agency Logo

The agency logo appears on audit trail PDFs and system-generated emails.

You can upload a logo file from a location available to the computer you are using to access Evidence.com.

- Logo file size must be less than five MB.
- The logo file type must be GIF, JPG, JPEG, BMP, TIF, or PNG.

You also have the option of deleting the logo.

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Agency Profile**.

   The Agency Profile page appears.

2. Click **Change Logo**.

3. If you want to specify a new logo, click **Choose File**, select the logo file, and click **Save**.

   The file uploads to Evidence.com.

4. If you want to remove the logo, click **Delete Logo**.
5. On the notification message box, click **OK**.

   The Agency Profile page shows the logo that you uploaded or, if you deleted the logo, shows a placeholder Evidence.com logo.

### Configure Agency Description

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Agency Profile**.

   The Agency Profile page appears.

2. Click **Edit Description**.

3. In the box provided, type the agency description.

4. When you finish updating the description, click **Save Changes**.

5. On the notification message box, click **OK**.

   The Agency Profile page displays the description that you provided.

### View Agency Audit Trail

The Agency Audit Trail shows agency-wide changes to your Evidence.com account. This report helps provide transparency on administrative actions across Evidence.com. By displaying each action in detail, your agency is able to review who changed a setting, in order to understand the purpose and provide better accountability to each user.

The audit trail logs the following Evidence.com changes:

- Device Default Ownership Policy Updated
- Address Added
- Address Updated
- Admin Added
- Admin Changed
- Authentication Policy Updated
- Partner Created
- Default Retention Level Updated
- Axon Body Settings Updated
- Flex Settings Updated
- Axon ATC Settings Updated
- Device Settings Updated
- X2 Settings Updated
- Dual Factor Authentication Policy Updated
- Expire All Subscriber Passwords of Partner Agency
- Partner Federation Entity Removed
- Partner Federation Entity Updated
- Federation Group Updated
- Partner Federation Updated
- Partner Federation Disabled
- IP Address Policy Updated
- IP Range Restriction Updated
- IP Address Session Security Policy Updated
- Password Policy Updated
- Agency Deactivated
- Agency Reactivated

Any user with the Edit Agency Settings permission Allowed under ADMIN ACCESS can view the Agency Audit Trail

1. On the menu bar, click Admin and then under Agency Settings, click Agency Profile. The Agency Profile page appears.

2. Click View Audit Trail. A dialog box provides options for viewing the entire audit trail or a portion of the audit trail.

3. If you want to view the whole audit trail, under View entire audit trail, click Submit.
4. If you want to view a portion of the audit trail, under View portion of audit trail, specify a date in either or both the From or To boxes, and then click Submit.

Evidence.com opens or downloads a PDF for the agency audit trail. The exact behavior depends on the browser you use and its download settings for PDF files.

5. Save or view the audit trail PDF as needed.

Field Validation

You can use the Field Validation feature to ensure that Evidence.com users enter information in the agency-defined format for specific fields. The feature lets administrators use a regular expression (regex) entry to set the expected format for the field and enter descriptor text to provide format information to users. When field validation is enabled, the descriptor text appears as hint text in the appropriate Evidence.com field and as part of the error message if the user does not enter the correct format.

Currently, you can enable field validation requirements for user Badge ID and Evidence ID. By default, both of these settings are not enabled.

Configure Field Validation

Administrators and users with roles that have the Edit Agency Settings permission set to Allowed can configure field validation.

Whether you are enabling a field validation for the first time or just updating the regular expression, the steps for configuring field validation are the same.

1. On the menu bar, click Admin and then click Field Validation.

The Field Validation page is shown.
2. Select the **Badge ID** and/or **Evidence ID** toggle switch to enable field validation.

3. For each field validation that is enabled:
   - In the **Regex** box, enter the regular expression that you want to use for field validation.
     
     See [Regular Expressions for Field Validation](#) for information and examples of regular expression notations.
   - In the **Descriptor** box, enter the text that you want to appear as hint text in field.
     
     See [User Experience](#) for an example of how the Descriptor text is used.
   - Click **Save**.

---

**Disable Evidence ID Validation**

Administrators and users who are allowed both the Category Administration and the Edit Agency Settings permissions can disable evidence ID validation as needed.
1. On the menu bar, click **Admin** and then click **Field Validation**.

2. Find the field validation you want to disable, **Badge ID** and/or **Evidence ID**, and select the toggle switch to disable field validation.

3. For each field validation that is disabled, click **Save**.

### Regular Expressions for Field Validation

Using standard Javascript regular expression notation, you can describe the format requirements your agency's fields. In order for a field entry to be valid, it must match the regular expression that you define.

The regular expression you specify must have a specific format.

- It must start with the following two characters: `/^`
- If you need field validation to be case **sensitive**, the regular expression must end with the following two characters: `$/`
- If you need field validation to be case **insensitive**, the regular expression must end with the following three characters: `$/i`
- Between the starting and ending characters, you provide a search pattern.

```
/^search-pattern$/
/^search-pattern$/i
```

The valid syntax for regular-expression search patterns is extensive and allows for great flexibility; however, if you are not already familiar with regular expressions, it is strongly recommended that you review Javascript regular expressions prior to implementing field validation in your Evidence.com agency.

For more information about Javascript regular expressions, see the following sites:

- Debuggex, a regular expression debugger site — [https://www.debuggex.com/](https://www.debuggex.com/)
Example Regular Expressions

The following table provides a few examples of ID formats and regular expressions that match only IDs that comply with the ID format.

<table>
<thead>
<tr>
<th>ID Format Example &amp; Description</th>
<th>Matching Regular Expressions and Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>YYYYMMDDnnnnnn</td>
<td>The following regular expression matches the YYYYMMDDnnnnnn format and requires that the ID begin with 20; however, it does not account for months with less than 31 days.</td>
</tr>
<tr>
<td>Four-digit year, two-digit month, two-digit day, and 6-digit number.</td>
<td>/^20\d\d\d(0[1-9]</td>
</tr>
<tr>
<td>YYYY-nnnnnn or YY-nnnnnn</td>
<td>The following regular expression allows any year between 2000 and 2099, with or without 20 at the start of the ID.</td>
</tr>
<tr>
<td>Four-digit year or two-digit year, a dash, and then a 6-digit number.</td>
<td>/(20)?(\d\d)-[0-9]{6}$/</td>
</tr>
<tr>
<td>XX-XXXX</td>
<td>The following regular expression requires that the ID begin with 2015; however, at the start of the new year, you would need to modify the regular expression.</td>
</tr>
<tr>
<td>Two characters, a dash, and then four characters.</td>
<td>/(20)?(15)-[0-9]{6}$/</td>
</tr>
<tr>
<td></td>
<td>The following regular expression allows any two alphanumeric characters, a dash, and then any four alphanumeric characters.</td>
</tr>
<tr>
<td></td>
<td>/[\w]{2}-[\w]{4}$/</td>
</tr>
</tbody>
</table>

User Experience

When adding or updating field information, users see hint text that reflects the field format requirements. For example, a user changing evidence IDs on an evidence search page sees the following dialog box:

![Image of dialog box](image)

If a user enters an evidence ID that does not match the regular expression configured for ID validation, Evidence.com does not allow the user to assign the ID to the evidence. In the
error message that appears, Evidence.com indicates that the ID is not valid and provides the hint text again.

![Invalid format for ID: 2112-123456
Expected format: Year-CaseNumber
UPDATE CANCEL]

Categories and Evidence Retention Policies

The Categories feature provides the ability to create policies, maintain them, and assign them to evidence. Categories include policy settings for evidence retention and restricted access for especially sensitive evidence.

Administrators or other users who are allowed the Category Administration permission can configure and delete categories.

Special and Pre-Configured Categories

Evidence.com includes two special categories:

- Uncategorized — Any evidence that is not assigned to another category is automatically assigned to the Uncategorized category. When you assign a category to evidence, it is automatically removed from the Uncategorized category.

- Pending Review

You cannot delete the Uncategorized or Pending Review category.

When your agency was created, we provided four additional categories that you can edit or delete as needed:

- Officer Injury
- Traffic Stop
- Training Demo
- Use of Force
Evidence Retention Policy

The evidence retention policy determines:

Whether Evidence.com initiates automatic deletion of evidence assigned to the category.

How long Evidence.com waits before initiating the deletion of evidence that is not included in a case. All evidence deletions are based on the recording date.

To protect against accidental deletions, administrators can recover files up to 7 days after they are queued for deletion.

This policy applies to evidence only. Cases are never deleted automatically.

Evidence included in a case is exempt from deletion until it is removed from the case.

If evidence is in multiple categories, the longest retention time is used.

Evidence.com sends the following notification emails about evidence queued for deletion:

- Administrators receive a weekly email that summarizes upcoming agency-wide deletions.
- Users receive a weekly message regarding evidence that they uploaded.

For administrators, the Dashboard includes an Upcoming Evidence Deletions section that lists both user-initiated and system-initiated deletions.

Restricted Categories

The Categories feature provides the ability to restrict access to evidence that is especially sensitive. In order to view evidence assigned to a restricted category, users must be on the evidence access list or assigned a role that has the Access Restricted Evidence permission.

By default, all new and pre-configured categories are not restricted categories.

By default, all new roles and all pre-configured roles have the Access Restricted Evidence permission set to prohibited.

Add a Category

You can create categories as needed. A new category has the following default settings:

- Evidence Retention — Until manually deleted
- Restricted Category — Not restricted
1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Retention Categories**.

   The Retention Categories page is shown.

2. Click **Add Category**.

   The New Evidence Category page appears.

3. Type a **Name** for the new category.

4. Under **Retention**, specify the retention duration for evidence in this category.

   - If you want Evidence.com to initiate deletion of evidence after a retention period, click the **Until Manually Deleted** list and select the unit of time. Then enter the length of the retention period.

   ![Retention Options](image)

   - If you do not want Evidence.com to initiate the deletion of evidence in this category, leave **Until Manually Deleted** as the selection.

5. Under **Restricted**, select if the new category is a restricted category. Enabling **Restrict** limits user access to users on the access list or with Access Restricted Evidence permission.

   - If you want the new category to be restricted, toggle the switch to **Restricted** (the toggle color is blue).

   - If you do not want the category to be restricted, leave the toggle at **Restrict** (the toggle color is white).

6. Click **Save**.

7. On the confirmation message box, click **Close**.
The Retention Categories page lists the category you added.

## Edit a Category

Before you edit a category, Axon recommends you search for all evidence that is assigned to the category and determine if, because the planned changes to the category, you should assign the evidence to a different category or an additional category.

If you change the retention period settings of a category, Evidence.com initiates deletion of any evidence assigned to the category that is older than the new retention period and which is not assigned to another category whose retention period dictates that the evidence be retained.

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Retention Categories**.

   The Retention Categories page appears.

2. Find the category you want to change and click the edit icon (✏️) on the same line as the category.

   The Edit Retention Category appears.

3. Edit the category as needed. For detailed steps, refer to the following table.

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the category name</td>
<td>Under <strong>Name</strong>, type the new name.</td>
</tr>
</tbody>
</table>
| Set a retention period for evidence assigned to this category | 1. Under **Retention**, select the unit of time for the category retention.  
2. In the box, type the length of the retention period. |
| Ensure that evidence in this category is retained indefinitely | Under **Retention**, select **Until Manually Deleted**.               |
| Restrict access to evidence assigned to the category | Under **Restricted**, toggle the switch to **Restricted** (the toggle color is blue). |
| Remove restrictions from access to evidence assigned to the category | Under **Restricted**, toggle the switch to **Restrict** (the toggle color is white). |

4. When you have finished editing the category, click **Update**.

5. If the “Category has been updated” notification message box appears, skip to step 9.

   A warning dialog box shows the number of evidence files affected by the changes to the category.
6. If you are not certain that the changes to the category are appropriate for all evidence currently assigned to the category, click Please review these evidence, review the category assignments of all the evidence files listed, and then repeat this procedure.

7. If you are certain that the changes to the category are appropriate for all evidence currently assigned to the category, click OK.

A confirmation message box displays information about acknowledging the possible effects of the changes to the category.

8. After you read the message, click OK.

9. In the notification message box, click Close.

Evidence.com saves the changes you made to the category and begins enforcing the effects of the changes.

**Delete a Category**

Before you delete a category, Axon recommends you search for all evidence that is assigned to the category and determine if you should assign the evidence to a different category or an additional category.

You can delete any category except for the following categories:

- Uncategorized
- Pending Review

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Retention Categories**.

   The Retention Categories page appears.

2. Find the category you want to delete and click the delete icon ( ) on the same line as the category.

   A dialog box lists the number of evidence files that are currently in the category you are deleting.

3. In the **Reassign Evidence to Category** list, select the category that you want to assign to the evidence files.

4. Click **Delete**.
5. On the confirmation message box, click **Close**.

   The Retention Categories page no longer lists the category you deleted.

---

**Device Settings**

Under Devices on the Admin portal page, administrators can access settings for the following features:

- Body Camera Settings
- Fleet Settings
- CEW Settings
- Vehicles
- Signal Configuration
- Signal Sidearm Registration
- Early Access Devices

---

**Configure Body Camera Settings**

The Body Camera Settings page enables agency administrators to define settings for Axon devices, such as Axon Body 2, Axon Body, Axon Flex, and Axon Flex 2. The page provides settings such as video quality, event pre-buffering, audio mute control, and indicator light control.

For additional information about Body Camera Settings, see the Body Camera Settings section of Appendix C.

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

Microphone controls are intended for agencies in locations with restrictions on audio recordings.

Video quality settings provide the ability to define the Axon video encoding rate or the space used per hour of recording. This is useful for agencies wanting to reduce the impact of Axon video uploads on the agency's Internet connection.
Note: To ensure that the quality of videos is acceptable, it is strongly recommended that you always validate the effect of the configured camera settings.

1. On the menu bar, click Admin, and then under Device Settings, click Body Camera Settings.

   The Body Camera Settings page displays sections for Axon Flex and Axon Body settings, Axon Body/Flex 2 settings, and settings affecting all Axon cameras.

2. For each setting, choose the option that best supports your agency’s policies regarding video, audio, and offline camera usage.

   For additional information about Body Camera Settings, see the Body Camera Settings section of Appendix C.

3. At the bottom of the page, click Save Settings.

   Evidence.com saves the camera settings. Axon Dock and Evidence Sync updates each camera with any changed settings the next time that the camera is connected.

Configure Fleet Settings

Fleet Settings configuration is only available to agencies that use Axon Fleet.

The Fleet Settings page is used to define default settings for Fleet system cameras. The page provides settings such as video quality, video pre-event buffering, audio mute control, and indicator light control.

For additional information about Fleet Camera Settings, see the Fleet Settings section of Appendix C.

Note: Some setting changes can only be enforced on each Axon Fleet camera after the camera is updated by Axon View XL or has been inserted in an Axon Dock or connected to an Evidence Sync application.

Video quality settings provide the ability to define the Axon video encoding rate or the space used per hour of recording. This is useful for agencies wanting to reduce the impact of Axon video uploads on the agency’s Internet connection.

Note: To ensure that the quality of videos is acceptable, it is strongly recommended that you always validate the effect of the configured camera settings.

1. On the menu bar, click Admin, and then under Devices, click Fleet Settings.
The Axon Fleet Settings page displays sections for settings affecting all Axon Fleet cameras for your agency.

2. For each setting, choose the option that best supports your agency's policies regarding video and audio usage.

For additional information about Fleet Camera Settings, see the Fleet Settings section of Appendix C.

3. At the bottom of the page, click **Save Settings**.

Evidence.com saves the camera settings.

## Configure CEW Settings

The CEW Settings page enables administrators to configure Conducted Electrical Weapons (CEW) Settings based on agency policy. Before you perform the following steps, ensure that you have installed Evidence Sync. For more information, see [Download and Install Evidence Sync](#).

1. On the menu bar, click **Admin** and then under **Devices**, click **CEW Settings**.

   The CEW Settings page appears.

2. As needed, configure the **CEW Auto-Shutoff Settings**, **Firing Mode Settings**, **Continued SPPM Transmit in Safe Setting**, and **Additional Settings** sections.

   **Note:** These settings are automatically applied to all the X2 and X26P devices assigned to your agency whenever those devices are next connected using the Evidence Sync application.
3. Click **Save**.

4. Launch the **Evidence Sync** (version 1.31.2836.20-2837 or higher) application. Connect an X2 or X26P device (version 3.033 or higher) to your computer using the USB cable. If connected through a TASER CAM HD, the camera must be version 0.30 or higher.

   The Device Summary page appears.
5. Click the **Device Settings** tab.

The CEW Settings options that were selected in your agency's Evidence.com account appear.

**Note:** These settings cannot be configured in Evidence Sync. To change any of the X2 and X26P device settings, you must sign in to your agency's Evidence.com administrator account and change them from the CEW Settings page.

---

**Signal Configuration**

Axon Signal is a technology that alerts your Axon Body 2, Axon Flex, Axon Flex 2, and Axon Fleet cameras to begin recording. With Axon Signal sending the alerts, officers can focus on critical situations rather than on their cameras.
Evidence.com administrators can configure which Axon Signal events will alert Axon body-worn and vehicle cameras for their agency. The Evidence.com Signal Configuration page is used to configure the events for the following Axon Signal products:

- **Axon Signal Vehicle**, the in-vehicle product, can report certain in-vehicle events, such as turning on a vehicle's light bar, to alert Axon cameras to begin recording.

- **Signal Performance Power Magazine (SPPM)**, an accessory for TASER X2 and X26P Smart Weapons, can report when a CEW is armed, when the trigger is pulled, and/or when the arc is engaged to alert Axon cameras to begin recording.

- **Axon Signal Sidearm**, a holster accessory, can report when a sidearm is drawn to alert Axon cameras to begin recording.

If no changes are made to the default Signal Configuration settings, then reports from Axon Signal products alert all body worn and Fleet vehicle front cameras to begin recording. If any changes are made to the Signal Configuration settings, then the body worn and Fleet cameras are alerted based on the settings.

### Configure Signal Vehicle Settings

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

**Example:** Axon Signal Vehicle is configured to alert body worn cameras and the Fleet front camera when a vehicle's light bar is turned on. When vehicle A turns on its light bar, the Fleet front camera in vehicle A and any body worn cameras within range are alerted to begin recording. But the front cameras in other vehicles are not.

1. On the menu bar, click **Admin** and then under **Devices**, click **Signal Configuration**.

   If you do *not* need to change the Signal Inputs configuration, skip to step 5.
2. Click the 🔄 icon to the right of **1 Signal Inputs**.

Under Signal Unit, the Signal Inputs area shows the inputs that are configured for Axon Signal Vehicle in your agency. Inputs 1 through 4 are reserved and cannot be configured.

3. For each input that you need to configure, from the input list, select the appropriate input.

4. When you have finished configuring inputs, click **Save and Continue**.

5. Click the 🔄 icon to the right of **2 Camera Activations**.

**Note:** The vehicle camera Front and Back settings are only available to agencies that use Axon Fleet.

6. For each input that you want to alert body-worn, Fleet Front, and Fleet Back cameras, move the corresponding switch to the right.

   If you want to configure all inputs to alert Axon cameras, move the **All** switch to the right.

7. Click **Save and Continue**.

Evidence.com saves your Axon Signal Vehicle settings.

---

**Configure CEW Signal Settings**

1. On the menu bar, click **Admin** and then under **Devices**, click **Signal Configuration**.

   Under CEW, the CEW Activations area shows the available events.
2. Click the icon to the right of **1 CEW Activations**.

   **Note:** The vehicle camera Front and Back settings are only available to agencies that use Axon Fleet.

3. For each event that you want to alert body-worn, Fleet Front, and Fleet Back cameras, move the corresponding switch to the right.

   If you want to configure all events to alert Axon cameras, move the **All** switch to the right.

4. Click the icon to the right of **2 Assigned Officer Activation**.

   **IMPORTANT:** To ensure the CEW Assigned Officer Activation setting functions as designed, your agency must ensure that SPPM-equipped CEWs and Axon Body Worn Cameras are correctly assigned and distributed to officers.

5. Move the Assigned Officer Activation switch as needed to enable or disable this capability.
When enabled, the Axon Signal transmission from a CEW only activates the Axon body worn camera assigned to the CEW user. When disabled, the Axon Signal transmission from a CEW activates any in-range Axon body worn camera.

This setting can only be used if your Axon cameras have firmware version 1.14 or later installed and your CEWs have the firmware version 4.037 or later installed.

6. Click **Save and Continue**.

Evidence.com saves your CEW Activations settings.

---

### Configure Signal Sidearm Settings

1. On the menu bar, click **Admin** and then under **Devices**, click **Signal Configuration**.

Under Signal Sidearm, the Signal Sidearm Activations area shows the available events.

![Signal Sidearm Activations](image)

2. Click the ✖️ icon to the right of **1 Signal Sidearm Activations**.

**Note:** The vehicle camera Front and Back settings are only available to agencies that use Axon Fleet.

3. Move the corresponding switch to the right to alert body-worn, Fleet Front, and Fleet Back cameras.

4. Click **Save and Continue**.

Evidence.com saves your Signal Sidearm Activations settings.

5. If you want to change the Signal Sidearm Mute Mode capability setting for your agency, click the ✖️ icon to the right of **2 Mute Mode Capability**.

6. Move the Mute Mode Capability switch as needed enable or disable Mute Mode capability.

When Mute Mode capability is enabled for your agency, officers can use the Signal Sidearm button to enter Mute Mode, which allows officers to remove their sidearm from their holster without alerting Axon cameras to record.
7. Click **Save and Continue**.

   Evidence.com saves Mute Mode Capability setting.

---

**Signal Sidearm Registration**

**Note:** Axon recommends using the Axon Device Manager Android app for registering and assigning Axon Signal Sidearm and other Axon devices.

Administrators manually record sensor serial numbers in Evidence.com and assign them to users. Administrators must make sure they accurately transcribe each sensor’s serial number.

**Note:** Serial numbers start with the letter “X” and are located on the back of the sensor. So, it is a best practice to register and assign units before they are installed on holsters.

---

**Register and Assign on Evidence.com**

1. Sign in to your Evidence.com account.

2. On the menu bar, click **Admin** and then under **Devices**, click **Signal Sidearm Registration**.

3. Enter the Signal Sidearm sensor Serial Number.
   
   Optional: Enter the name or badge number of the person you want to assign the sensor to in the **Assignee** field.

4. Click **Register Device**.
Early Access Devices

Early Access Devices are an optional way for an agency to set up Axon Body 2 cameras, Axon Flex 2 cameras, Axon Flex 2 controllers, and Axon Docks as test devices that receive firmware updates before the general release of the updates. Axon is confident in the quality of our validation and release process. This option is designed to provide agencies with the opportunity to review and test the changes in their own environment on a small scale before full deployment.

Note: You must have Axon Dock firmware v3.6 or higher to use early access devices.

If your agency chooses to use this option, your administrators will receive an email informing them about the upcoming early access firmware update. When the update is deployed, only devices specified by your agency will receive the early firmware update. You can have up to 15 of each device type specified as early access devices. Axon recommends that you regularly test your early access devices to ensure the firmware updates do not impact your current processes. Additionally, you should control access and deployment of these devices, since the firmware version for the devices can be out of synchronization with other devices at your agency.

If your agency finds problems with a firmware update during testing, please contact Technical Support and let them know that you are having an issue with an early access device.

Add a Device to the Early Access List

1. On the menu bar, click Admin, and then under Device, click Early Access Devices.

2. Find the type of device (Axon Body 2, Axon Dock, Axon Flex 2, or Axon Flex 2 Controller) you want to add.

3. Click Add Device.

4. Enter the device serial number and click Save.
### Remove a Device from the Early Access List

1. On the menu bar, click **Admin**, and then under **Device**, click **Early Access Devices**.

2. Find the device you want to remove from the early access device list.

3. Click ✖️ (delete), the device is removed from the list.
Security Settings

Under Security Settings on the Admin portal page, administrators can access settings related to site security.

IP Security

By enabling the IP Security, agency administrators can define who is allowed or not allowed to access their agency's Evidence.com accounts based on the IP address. By default, when your Evidence.com agency is created, IP security is disabled and your agency's sign-in page can be accessed from anywhere within your country.

If you enable IP security, you can authorize specific IP addresses and ranges of IP addresses, such as the IP addresses used at your agency headquarters or at specific districts. Only devices assigned one of the authorized IP addresses can access your Evidence.com agency.

Note: Before you enable IP security, work with your IT staff and your Internet provider to acquire static (non-changing) IP addresses. If you do not use static IP addresses, your agency could be denied access from its own Evidence.com agency. Consumer-grade Internet lines, such as DSL or cable modems, typically have a 200-hour lease. This means that every 200 hours the IP address is refreshed with a new one.

1. On the menu bar, click Admin and then under Security Settings, click IP Address.

   The IP Active Session Security area appears at the top of the page.

2. To enable IP Address Security, under the Add a New IP Address section in the IP Address field, enter the known IP address or default gateway that is seen by the Internet for your agency. You must enter a Starting and Ending IP Address if you select Range of IP Address.

3. Enter a useful description of this address in the Label field. The Label field is optional, but descriptive labels help make managing your Evidence.com account easier.

4. Click Add Allowed IP Address to add the location.

   The newly added IP Address shows in the table.

5. You can continue adding additional IP Addresses as required.

6. Select the Restrict User Access to the Trusted IP Addresses Below checkbox located at the top of the page.
Note: You cannot select this option unless at least one IP address or range of IP addresses has been added.

7. If at any time you want to prevent access from any IP addresses, click the corresponding Delete link. However, to prevent being locked out of your account ensure that you do not delete your current IP address.

IP Whitelisting for Multi-Homed Networks

Evidence.com supports IP security whitelists for agencies where web traffic can originate from multiple IPs during the same user session. The standard IP whitelist security detects if an active user changes source IP address in the middle of a session and logs the user out. The new setting still restricts site usage to the IP whitelist ranges, but does not terminate a user session if there is an IP change mid-session.

This setting is designed for agencies using network designs where web traffic is sourced from multiple IPs. For example, networks with multiple firewalls or proxy servers can exhibit this behavior. Agencies that load balance outbound traffic across multiple network links also fall into this category. These designs are perfectly valid but cause a false positive for our “Man in the Middle” protection. Until now, these agencies have not been able to utilize our IP whitelist security.

If your agency is not using this type of design, it is recommended that you employ the standard IP session security for the highest levels of protection.

1. On the menu bar, click Admin and then under Security Settings, click IP Address.

2. Under the Add a New IP Address section in the IP Address field, enter the known IP address. You must enter a Starting and Ending IP Address if you select Range of IP Address.

3. Enter a useful description of this address in the Label field. The Label field is optional, but descriptive labels help make managing your Evidence.com account easier.

4. Click Add Allowed IP Address to add the location.

The newly added IP Address shows in the table.

5. Select the Allow IP Address To Change During An Active Session To The Trusted IP Addresses Below check box.
Multi-Factor Authentication

Multi-Factor Authentication requires all Evidence.com administrators and users with critical action permissions to use multi-factor authentication when signing in and when completing critical actions. It adds a layer of security to ensure an agency's most powerful Evidence.com user accounts are secure and protected from malicious attacks.

Note: If your agency uses Single Sign-On (SSO) functionality, then multi-factor authentication is disabled by default. If needed multi-factor authentication can be enabled for SSO agencies. Contact your Axon representative for more information.

After a user makes a critical change, Evidence.com asks them to enter a security code. The security code is sent to the user's mobile phone or email address, depending on the Multi-Factor Authentication settings for your agency. In cases where your agency delivery method setting is set to send to the user's mobile phone and the user does not have a verified phone number listed in their user information, the system will automatically send a security code to the user's email address.

After the user enters the security code, the action is completed. Further authentication is not required for other critical actions taken within the number of minutes specified in the account settings.

Additionally, when signing in to Evidence.com, there are some cases (such as signing in from a new IP address) where users with critical action permissions are asked to enter a security code to complete their sign in.

You can also enable multi-factor authentication for all users in your agency. If enabled agency-wide, the standard security question authentication is replaced with a multi-factor authentication when any user signs in or makes a critical change.

Critical Action Permissions

Users that are assigned a Role with critical action permissions are required to use multi-factor authentication when signing in and when they make a change associated with the permission. The following permission settings are considered critical action permissions for multi-factor authentication:

- Configure Agency Security Settings = Allowed
- Edit Agency Settings = Allowed
- Edit Device Offline Microphone Settings = Allowed
- User Administration = Allowed
• Category Administration = Allowed
• Delete Evidence & Edit Date Recorded = Any Evidence
• Access Restricted Evidence = Allowed

**Multi-Factor Authentication Account Settings**

To set or change the Multi-Factor Authentication settings for your agency:

1. On the menu bar, click **Admin** and then under **Security Settings**, click **IP Address**.
2. Scroll down to the Multi-Factor Authentication settings section below the IP Active Session Security settings.
3. Select if Multi-Factor Authentication will apply **Agency-Wide** or for **Admin Only** users.

   The Agency-Wide setting requires all users to enter a security code delivered by phone or email when they sign in to Evidence.com or when they make a critical change.

   The Admin Only setting only requires users assigned to Roles with critical action permissions to enter a security code when they sign in or when they make a critical change. All other users will continue to be prompted with security questions.

4. Choose the delivery method for the security codes; **SMS Text** or **Automated Call Back** or **Email**.

   Axon recommends using SMS Text, since using a mobile phone is normally the fastest method for receiving the security code.

5. Enter how long, in minutes, the security code is valid in Evidence.com in the **Security Challenge Frequency** field. After the codes expire, users are prompted to enter new codes. The value can be any whole number from 2 to 20 minutes.

6. Click **Save**.

   Your agency’s Multi-Factor Authentication Settings are now configured.

**Configure Password Settings**

This feature enables administrators to define password settings for all users in the agency.

• **Password History** — Unique new passwords a user must use before an old password can be reused. [default 10, min 1, max 25]
• **Password Aging** — Determines how many days a password can be used before the user is required to change it. [default 90, min 7, max 365]

• **Password Length** — Determines how short passwords can be. [default 8, min 6]

• **Failed Login Limit** — Number of failed login attempts before the account is locked out. [default 5, min 1, max 25]

• **Lockout Duration** — Number of minutes a user is locked out of their account due to failed login attempts. [default 60, min 1, max 720]

• **Session Timeout** — Number of minutes a user can be inactive before the user is automatically signed out of Evidence.com. [default 15, min 15, max 480]

**Note:** There are no configuration settings for user security questions. Users have 15 attempts to enter their correct security question responses. Users that fail to enter the correct security question responses are locked out of the system for 1 hour.

1. On the menu bar, click **Admin** and then under **Security Settings**, click **Password Configuration**.

   The Password Configuration page with the various settings appears. Below each setting are a description and the default and maximum (max) values of the setting.

2. Set the options based on your agency’s requirements.

   **Note:** If you want to start over with customizing the password configuration settings, click **Restore Defaults**.

3. When have finished configuring password settings, click **Save**.

4. On the notification message box, click **OK**.

---

### API Settings

Available to Evidence.com agencies who request access to the Evidence.com Partner API, the API Settings page provides administrators the ability to ensure that only authenticated and authorized clients can use the Partner API feature to programmatically configure your Evidence.com agency. The Partner API supports the use of third-party programmatic clients to perform create, read, update, and delete operations on the resources supported by the API, which include the following object types:

- Users
- Groups
Cases

Evidence

Devices

Reports

For more information, please contact your Axon representative or send inquiries to Axon Technical Support at support@axon.com.

**Partner Agency Administration**

Evidence.com makes it easy for your users to share evidence and cases with other Evidence.com agencies. The agencies you share with or who share with you are *partner agencies*. Partner agencies have access only to data that you specifically share with them. All unshared data owned by your agency remains completely unavailable to partner agencies.

**Partner Agency Lists**

In the Admin section of your Evidence.com agency, the Partner Agencies page has two lists that administrators can use to control how your agency collaborates with its partner agencies.

- **Agencies In My Contacts** — The agencies whose users and groups are available for your agency to share with. These agencies invited you to view their user and group lists. They have added your agency to their Agencies With My Contacts list.

  When a user in your agency wants to share cases and evidence with a partner agency, the users and groups of these agencies are available and can be found when your user searches for people to share with.

<table>
<thead>
<tr>
<th>AGENCIES IN MY CONTACTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agency</strong></td>
</tr>
<tr>
<td>District Attorney</td>
</tr>
</tbody>
</table>

- **Agencies With My Contacts** — The agencies that can share with your users and groups. These agencies accepted your invitation to view your directory. They have accepted your invitation and your agency appears on their Agencies In My Contacts list.
When a user in one of these agencies wants to share cases and evidence with your agency, the users and groups of your agency are available and can be found when the user in the other agency searches for people in your agency to share with.

<table>
<thead>
<tr>
<th>AGENCY</th>
<th>CITY</th>
<th>STATE</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>District Attorney</td>
<td>Seattle</td>
<td>Washington</td>
<td>Accepted</td>
</tr>
<tr>
<td>Police Squad</td>
<td>Seattle</td>
<td>Washington</td>
<td>Awaiting Acceptance</td>
</tr>
</tbody>
</table>

**Sharing with Partner Agencies**

Users who are allowed the Share with Partner Agencies permission can share cases with agencies on your Agencies In My Contacts list. Users who are allowed the Share Externally to Authenticated Users permission can share evidence with agencies on your Agencies In My Contacts list.

For more information about sharing with partner agencies, see the following topics:

- Share an Evidence File
- Bulk Share Evidence by Authenticated Sharing
- Share a Case by Download Link
- Share a Case with a Partner Agency

**Invite an Agency to Share with Your Agency**

In order to allow your users to share cases and evidence with another agency, you must invite the other agency. When you invite an agency, you are sharing your agency’s contact list with that agency. Your contact list consists of the following items:

- All your users.
- Your groups that have the “Allow Partner Agencies to share with this group” setting enabled. For more information, see Groups Receiving Shared Cases from Partner Agencies.

**Note:** Administrators of agencies that you add to your Agencies With My Contacts list receive a notification email. Before you can share a case with the partner agency, an administrator from the partner agency must accept the invitation to collaborate with your agency.
1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Partner Agencies**.

   The Partner Agencies page appears.

2. Under **Agencies With My Contacts**, click **Add Agency**.

   An agency-search dialog box opens.

3. Search for the agency that you want to allow to share cases and evidence with your agency.

4. In the search results, click the agency name.

5. On the confirmation message box, click **OK**.

   The agency appears in the Agencies With My Contacts list, with the status “Awaiting Acceptance”. Administrators of the new partner agency receive an email notifying them of the invitation to receive shared cases and evidence from with your agency.

6. On the notification message box, click **OK**.

   After the partner agency has accepted the request to collaborate with your agency, users of your agency who have permission to share with partner agencies can share with the new partner agency.

---

**Accepting or Rejecting an Invitation to Collaborate with an Agency**

When another agency adds your agency to their Agencies With My Contacts list, Evidence.com sends a notification email to administrators of your agency. Before the other agency can share cases and evidence with your agency, you must accept the invitation.

Alternatively, if you do not want to allow the other agency to collaborate with your agency, you can reject the invitation.

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Partner Agencies**.

   The Partner Agencies page appears.

2. In the **Agencies In My Contacts** list, find the agency who invited you to collaborate.

3. Do one of the following:
   - If you want to allow your users to share evidence and cases with the other agency, click **Accept**.

   Your agency can now share cases and evidence with the other agency.
Administrators of the partner agency receive notification emails that you accepted the invitation to collaborate.

- If you do not want to allow your users to share cases and evidence with the other agency, click Reject and then, on the confirmation dialog box, click OK.

# Ending Collaboration with a Partner Agency

If you no longer want to collaborate with a partner agency, remove that agency from the applicable lists on the Partner Agencies page.

<table>
<thead>
<tr>
<th>Task</th>
<th>Steps</th>
</tr>
</thead>
</table>
| Prevent a partner agency from sharing cases and evidence with your users. | 1. On the menu bar, click Admin and then under Agency Settings, click Partner Agencies.  
2. In the Agencies With My Contacts list, find the agency and click the corresponding X button.  
3. On the confirmation message box, click OK.  
4. On the notification message box, click OK.  
Your agency can no longer receive shared cases and evidence from the other agency. |

| Prevent your agency from sharing cases and evidence with a partner agency. | 1. On the menu bar, click Admin and then under Agency Settings, click Partner Agencies.  
2. In the Agencies In My Contacts list, find the agency and click the corresponding X button.  
3. On the confirmation message box, click OK.  
4. On the notification message box, click OK.  
Your agency can no longer send shared cases and evidence to the other agency. |
Active Directory—Single Sign On

The Active Directory—Single Sign On feature is an Early Access feature and does not appear in your agency account unless you request access. In order to join the program and gain access to this feature, contact your local Axon representative or email Technical Support at support@axon.com.

Evidence.com can interface with a federated Active Directory to allow users to log in with their agency credentials.

Using the industry-standard SAML protocol, your officers no longer need to juggle multiple usernames and passwords. With Active Directory federation, Evidence.com uses your network to authenticate users. Your agency credentials are never sent to Evidence.com.
Help Section

All Evidence.com users can access the Help section to view release notes and user guides; to download Evidence Sync and Axon Capture; or to contact us with questions or comments.

Help Center

We are in the process of updating the Evidence.com Help Center page. In the meantime, we recommend you visit the Evidence.com section of the Axon Help Center for information about the various features of Evidence.com and of Evidence Sync.

Release Notes and User Guides

The Notes and Guides page displays links to the Evidence.com release notes and user guides.

The Release Notes section lists the release notes for each previous version of Evidence.com, in reverse chronological order.

The User Guides sections displays links to the most recent version of the available guides.

Release notes and user guides are in PDF format.

1. On the menu bar, click Help and then click Release Notes / User Guides.

   The Release Notes and User Guides sections list links to the various documents.

2. To access a document, click a link.

   Evidence.com opens or downloads a PDF. The exact behavior depends on the browser you use and its download settings for files.

Download and Install Evidence Sync

You can download the current version of the Evidence Sync application from the Downloads page. Using Evidence Sync for Windows, you can manage and upload data from your TASER X2, TASER X3, TASER X26, TASER X26P, TASER CAM, TASER CAM HD, Axon Flex, Axon Body, Axon Body 2, and Axon Flex 2 devices to Evidence.com.

Note: The videos recorded on Axon Flex system can be uploaded to the device owner's Evidence.com account by using Evidence Sync software version 1.30.2307 and above.
1. On the menu bar, click **Help** and then click **Download Sync**.

   The Evidence Sync installer .EXE file begins downloading.

2. Save the EXE file in a convenient location.

3. After the EXE file has finished downloading, run the file.

4. If a User Account Control window appears, click **Yes**.

   The Select Setup Language dialog box appears.

5. In the list, click the language you want to use and then click **OK**.

   The Welcome to the Sync Setup Wizard window appears.

6. Click **Next**.

7. Review the License Agreement

8. Click **I accept the agreement** and then click **Next**.

9. Choose the installation location. It is recommended that you maintain the displayed default location.

10. Click **Next**.

11. Choose the Start Menu folder where you want the Sync shortcut to appear and then click **Next**.

12. If you want the installation software to create desktop icon for the Sync application, select the corresponding check box.

13. If you use Sync with TASER X3 CEWs, select the corresponding check box.

14. Click **Next** and then click **Install**.

   The installation begins.

15. When the installation is complete, click **Finish**.

   The Evidence Sync application starts automatically.
**Download Axon Capture**

Axon Capture allows users to capture and upload photos, videos, and audio, and to add tags, titles, and location information about the captured files.

Axon Capture is supported on mobile devices that run Apple iOS and Google Android.

1. On the menu bar, click **Help** and then click **Download Mobile App**.

   A dialog box provides several ways for you to access installation information: text message, email, the Apple AppStore web site, or the Google Play web site.

2. Select the method you want to use to access installation information.

3. Click **Close**.

4. Use the method you selected to install the app on your mobile device.

**Download Evidence Upload XT**

Evidence Upload XT is a Windows-based desktop application that enables users to easily upload non-Axon generated digital evidence to their agency's Evidence.com account. This makes it easier to use Evidence.com as your central Digital Evidence Management system (DEMs).

Evidence Upload XT has the following minimum system requirements:

- Windows 7 operating system
- 2 GB RAM
- Internet access with the ability to reach Evidence.com

To download Evidence Upload XT:

1. Sign in to your Evidence.com account, go to the Help tab, and then click **Download Evidence Upload XT** to download the latest version of installation file.

2. Double-click the Evidence Upload XT installation file and follow the on-screen instructions.

3. When the installation is complete, an Evidence Upload XT icon is added to your desktop and to the list of programs in the Start menu.
Contact Us

The Contact Us page displays contact information. If you or your agency’s Evidence.com users have any questions or queries regarding our products and services, you can contact us using the options listed on this page.

1. On the menu bar, click Help and then click Contact Us.

2. From the lists provided, select the topic you need help with and select how you prefer to be contacted.

3. Provide your contact information.

4. In the Message box, type your question. Please be specific, to help ensure that we can provide you an accurate and precise response.

5. Click Submit.

6. On the notification message box, click OK.
Appendix A: Roles and Permissions

This appendix provides additional information about the Roles and Permissions feature. Roles determine user permissions, which control the user’s access to features and functions. Each Evidence.com user is assigned a role. For more information about using this feature, see Roles and Permissions.

Administrators and users whose role has the Edit Agency Settings permission set to Allowed can create and edit roles. Administrators and users whose role has the User Administration permission set to Allowed can assign roles to users.

By default, Evidence.com provides all agencies with pre-configured roles and locked roles. Locked roles cannot be changed by your agency.

<table>
<thead>
<tr>
<th>Pre-Configured Role</th>
<th>Locked or Configurable</th>
<th>Required License Tier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>Locked</td>
<td>Pro</td>
</tr>
<tr>
<td>User</td>
<td>Configurable</td>
<td>Basic (Pro if a Pro license permission is allowed)</td>
</tr>
<tr>
<td>Investigator</td>
<td>Configurable</td>
<td>Pro</td>
</tr>
<tr>
<td>Armorer</td>
<td>Configurable</td>
<td>Basic (Pro if a Pro license permission is allowed)</td>
</tr>
<tr>
<td>Lite User</td>
<td>Locked</td>
<td>N/A</td>
</tr>
<tr>
<td>Lite Armorer</td>
<td>Locked</td>
<td>N/A</td>
</tr>
</tbody>
</table>

The Lite User and Lite Armorer roles are designed for users that only work with TASER Conducted Electrical Weapons (CEW) logs and TASER CAM videos. The Lite Armorer role acts as a CEW administrator and can reassign agency CEW devices, change CEW settings, and upload any CEW logs.

For more information about the permissions associated with each pre-configured role, see the Pre-Configured Roles section.

Permission Reference

The following table provides information about each permission supported by Evidence.com. The Unlocked By column indicates if other permissions must be allowed in order for a permission to be available for you to configure.
<table>
<thead>
<tr>
<th>Permission</th>
<th>Requires Pro License?</th>
<th>Unlocked By:</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Login Access</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evidence.com</td>
<td>No</td>
<td>—</td>
<td>Allows a user to log in to their agency’s Evidence.com agency.</td>
</tr>
<tr>
<td>Evidence Sync</td>
<td>No</td>
<td>—</td>
<td>Allows a user to log in to Evidence Sync in Online mode.</td>
</tr>
<tr>
<td>Axon Capture</td>
<td>No</td>
<td>—</td>
<td>Allows a user to log in to the Axon Capture mobile application.</td>
</tr>
<tr>
<td>Axon View XL</td>
<td>No</td>
<td>—</td>
<td>Allows a user to log in to Axon View XL.</td>
</tr>
<tr>
<td><strong>User Account</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit Account Information</td>
<td>No</td>
<td>—</td>
<td>Allows a user to change their own account information, including their Name, Badge ID, Phone, Email Address, Password, Security Questions, or Email Settings. If you change the User Administration permission to Allowed, this permission is automatically set to Allowed.</td>
</tr>
<tr>
<td>View &amp; Compose User Messages</td>
<td>No</td>
<td>User Search</td>
<td>Allows a user to read and send messages to other users.</td>
</tr>
<tr>
<td>Download Sync Software</td>
<td>No</td>
<td>—</td>
<td>Allows a user to download Sync software from their Evidence.com agency.</td>
</tr>
<tr>
<td>Create/Edit Group</td>
<td>No</td>
<td>User Search</td>
<td>Allows a user to create a group, and edit its monitors and members.</td>
</tr>
<tr>
<td>Group Audit Trail PDF</td>
<td>No</td>
<td>—</td>
<td>Allows a user to view an audit trail of the activities related to a group.</td>
</tr>
<tr>
<td><strong>Admin Access</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure Agency Security Settings</td>
<td>No</td>
<td>—</td>
<td>Allows a user to edit the agency's IP Restrictions, authentication method, password configurations, partner agencies, and transcription accounts.</td>
</tr>
<tr>
<td>Edit Agency Settings</td>
<td>No</td>
<td>—</td>
<td>Allows a user to configure agency wide settings including Field Validation, Retention Categories, Video and Camera Settings, Roles and Permissions, and Password Configuration requirements.</td>
</tr>
<tr>
<td>Edit Device Offline &amp; Microphone Settings</td>
<td>No</td>
<td>Edit Agency Settings</td>
<td>Allows a user to configure the agency-wide settings for the Axon cameras default Microphone Setting and whether or not they can be turned to Offline Mode.</td>
</tr>
<tr>
<td>CEW Administration</td>
<td>No</td>
<td>User Search, Device Search, View CEW Firing Logs</td>
<td>Allows a user to search for reassign agency CEW and TASER CAM devices, change settings, and upload any CEW logs.</td>
</tr>
<tr>
<td>Permission</td>
<td>Requires Pro License?</td>
<td>Unlocked By:</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------</td>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Device Administration</td>
<td>No</td>
<td>User Search and Device Search</td>
<td>Allows a user to reassign all agency non-CEW devices and change their settings.</td>
</tr>
</tbody>
</table>
| User Administration         | No                    | User Search                  | Allows a user to add, remove and edit the accounts of other users, including their role, personal information, contact information, and reset their credentials (password and security questions).  
**Important:** Users with this permission can create users with full administrative privileges. |
<p>| Category Administration     | No                    | —                             | Allows a user to add a Category to the agency’s list or edit an existing Category.                                                               |
| Generate Reports            | Yes                   | —                             | Allows a user to generate reports.                                                                                                             |
| <strong>Search Access</strong>           |                       |                               |                                                                                                                                             |
| User Search                 | No                    | —                             | Allows a user to see what users are in the agency. If disabled the user are unable to see any evidence or devices assigned to others, assign devices or evidence to others, share evidence or cases, or send messages to others. |
| Partner Contact Search      | No                    | —                             | Allows a user to view members of partner agencies that have been added to your agency’s contact list.                                             |
| Evidence Search             | No                    | User Search                  | Allows a user to search for all of the Evidence in the agency. Note: the user can only access the Evidence specified under the Evidence Management permissions. |
| Device Search               | No                    | User Search                  | Allows a user to search for all of the Devices in the agency.                                                                                   |
| Case Search                 | No                    | User Search and Evidence Search | Allows a user to search for all of the Cases in an agency. Note: Their ability to access a Case is determined by the Case Management Permissions. |
| <strong>Evidence Creation</strong>       |                       |                               |                                                                                                                                             |
| Upload External Files       | No                    | —                             | Allows a user to upload files through Evidence Sync, Axon Capture, and the Import Evidence feature. This does not affect the ability to upload through Axon Dock. |
| Configure Automatic Upload through Evidence Sync | No | Upload External Files | Allows a user to configure Automatic Upload through Evidence Sync. |</p>
<table>
<thead>
<tr>
<th>Permission</th>
<th>Requires Pro License?</th>
<th>Unlocked By:</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Evidence Management</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View</td>
<td>No</td>
<td>—</td>
<td>Allows a user to access evidence, except for weapon firing logs. Can be set to allow access to any evidence or only the user’s evidence.</td>
</tr>
<tr>
<td>View CEW Firing Logs</td>
<td>No</td>
<td>—</td>
<td>Allows a user to access, edit, and download weapon firing logs and TASER CAM videos. It also allows a user to view and download the audit trail for the weapon firing logs. This can be set to allow access to any weapon logs or only the user’s weapon logs. Evidence Search must be set to Allowed to allow the user to access any weapons logs.</td>
</tr>
<tr>
<td><strong>Edit</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit</td>
<td>No</td>
<td>Evidence Management View</td>
<td>Allows a user to change the Title, ID, Flag, Assignment, Category, Tags, Location, Clips, and Markers. Can be set to allow access to any evidence or only the user's evidence.</td>
</tr>
<tr>
<td>Add/Remove Pending Review Category</td>
<td>No</td>
<td>Evidence Management Edit</td>
<td>Allows a user to add or remove the Pending Review Category from a piece of Evidence. Can be set to allow access to any evidence or only the user's evidence.</td>
</tr>
<tr>
<td><strong>Redact</strong></td>
<td>Yes</td>
<td>Evidence Management Edit</td>
<td>Allows a user access to the tools in the redaction suite, such as manual redaction, bulk redactions and Smart tracker technology. Can be set to allow access to any evidence or only the user's evidence.</td>
</tr>
<tr>
<td>Order Transcript</td>
<td>Yes</td>
<td>Evidence Management View</td>
<td>Allows a user to order transcripts.</td>
</tr>
<tr>
<td>Reassign</td>
<td>No</td>
<td>User Search and Evidence Management View</td>
<td>Allows a user to change the owner of a piece of evidence. Can be set to allow access to any evidence or only the user's evidence.</td>
</tr>
<tr>
<td>Delete Evidence &amp; Edit Date Recorded</td>
<td>No</td>
<td>Evidence Management View</td>
<td>Allows a user to manually initiate the deletion of Evidence before its Category determined date. Can be set to allow access to any evidence or only the user's evidence.</td>
</tr>
<tr>
<td>Download</td>
<td>No</td>
<td>Evidence Management View</td>
<td>Allows a user to download Evidence. Can be set to allow access to any evidence or only the user’s evidence.</td>
</tr>
<tr>
<td>Download Infected Files</td>
<td>No</td>
<td>Evidence Management Download</td>
<td>Allows a user to download Evidence that either failed a malware scan or is currently being scanned.</td>
</tr>
<tr>
<td>Permission</td>
<td>Requires Pro License?</td>
<td>Unlocked By:</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------</td>
<td>---------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Share</td>
<td>No</td>
<td>User Search and Evidence Management View</td>
<td>Allows a user to add other users to the access list for evidence. Can be set to allow this action for any evidence or only the user’s evidence.</td>
</tr>
<tr>
<td>Restrict</td>
<td>No</td>
<td>Evidence Management View and Evidence Management Share</td>
<td>Allows users to restrict the access list for evidence. Can be set to allow this action for any evidence or only the user’s evidence.</td>
</tr>
<tr>
<td>Share Externally to Authenticated Users</td>
<td>No</td>
<td>Partner Contact Search, Evidence and Management Share</td>
<td>Allows users to provide individuals outside of your agency with access to evidence. These external users are required to sign in to their Evidence.com account to view the shared evidence, and their actions are shown in your agency’s audit trails. If they do not have an Evidence.com account, they can create a free guest account on my.evidence.com.</td>
</tr>
<tr>
<td>Share External Download Links</td>
<td>No</td>
<td>Evidence Management Share and Evidence Management Download</td>
<td>Allows users to send an email containing a download link to individuals outside of your agency. This link does not require the recipient to sign in to an Evidence.com account or even to have an Evidence.com account. Only the apparent IP address of the computer downloading the file appears in your agency’s audit trails.</td>
</tr>
<tr>
<td>Post Notes</td>
<td>No</td>
<td>Evidence Management View</td>
<td>Allows a user to write messages associated with Evidence. Can be set to allow access to any evidence or only the user’s evidence.</td>
</tr>
<tr>
<td>Audit Trail PDF</td>
<td>No</td>
<td>Evidence Management View</td>
<td>Allows a user to view and download the record of who has Viewed or Edited Evidence. Can be set to allow access to any evidence or only the user’s evidence.</td>
</tr>
<tr>
<td>Access Restricted Evidence</td>
<td>Yes</td>
<td>Evidence Management View</td>
<td>This permission setting allows users to access all restricted evidence inside your agency without being on the evidence’s Access List. This permission requires that Evidence Management View be allowed for the associated role.</td>
</tr>
</tbody>
</table>

**Case Management**

<table>
<thead>
<tr>
<th>Permission</th>
<th>Requires Pro License?</th>
<th>Unlocked By:</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>No</td>
<td>—</td>
<td>Allows a user to access a Case. Can be set to allow access to any case or only the user’s cases.</td>
</tr>
<tr>
<td>Edit</td>
<td>No</td>
<td>Case Management View</td>
<td>Allows a user to Edit Case ID, Description, Categories, Tags, and Folder Structure. Can be set to allow access to any case or only the user’s cases.</td>
</tr>
<tr>
<td>Permission</td>
<td>Requires Pro License?</td>
<td>Unlocked By:</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------</td>
<td>--------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reassign</td>
<td>No</td>
<td>User Search and Case Management Edit</td>
<td>Allows a user to change the Owner of a piece of a Case. Can be set to allow access to any case or only the user's cases.</td>
</tr>
<tr>
<td>Share</td>
<td>No</td>
<td>User Search and Case Management Edit</td>
<td>Allows a user to add members to a Case, giving them access to the associated evidence. Can be set to allow access to any case or only the user's cases.</td>
</tr>
<tr>
<td>Share with Partner Agencies</td>
<td>No</td>
<td>Partner Contact Search, Case Management Share, and Evidence Management Share</td>
<td>Allows users to send cases to a partner agency. After the partner agency accepts the case, the evidence in the case is copied to the partner agency and no further actions by the partner agency are shown in your agency's audit trails.</td>
</tr>
<tr>
<td>Share External Download Links</td>
<td>No</td>
<td>Case Management Share and Evidence Management Share External Download Links</td>
<td>Allows users to send an email containing a download link to individuals outside of your agency. This link allows recipients to download all of the evidence in the case. Using the link does not require recipients to sign in to an Evidence.com account or even to have an Evidence.com account. Only the apparent IP address of the computer downloading the file appears in your agency's audit trails.</td>
</tr>
<tr>
<td>Audit Trail PDF</td>
<td>No</td>
<td>Case Management View</td>
<td>Allows a user to view and download the record of who has Viewed or Edited a Case. Can be set to allow access to any case or only the user's cases.</td>
</tr>
<tr>
<td>View &amp; Add Case Notes</td>
<td>No</td>
<td>Case Management View</td>
<td>Allows a user to write messages associated with a Case. Can be set to allow access to any case or only the user's cases.</td>
</tr>
<tr>
<td>Create Case</td>
<td>No</td>
<td>Evidence Management Search and Case Management View</td>
<td>Allows a user to create a Case.</td>
</tr>
<tr>
<td>Restricted Category Access</td>
<td>No</td>
<td>Case Management View</td>
<td>Allows a user to access Cases that have been categorized as Restricted Access.</td>
</tr>
<tr>
<td><strong>Shared Case</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View</td>
<td>No</td>
<td>—</td>
<td>Allows users to access a Case that has been Shared with them.</td>
</tr>
<tr>
<td>Permission</td>
<td>Requires Pro License?</td>
<td>Unlocked By:</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-----------------------</td>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Edit</td>
<td>No</td>
<td>Shared Case View</td>
<td>Allows users to Edit Case ID, Description, Categories, Tags, and Folder Structure of a Case that has been shared with them.</td>
</tr>
<tr>
<td>Reassign</td>
<td>No</td>
<td>Shared Case View and User Search</td>
<td>Allows a user to reassign a Case that has been Shared with them.</td>
</tr>
<tr>
<td>Share</td>
<td>No</td>
<td>Shared Case View and User Search</td>
<td>Allows users to add members to a Case that has been shared with them, giving access to the associated Evidence.</td>
</tr>
<tr>
<td>View &amp; Add Case Notes</td>
<td>No</td>
<td>Shared Case View</td>
<td>Allows users to write messages associated with a Case that has been Shared with them.</td>
</tr>
<tr>
<td>Audit Trail PDF</td>
<td>No</td>
<td>Shared Case View</td>
<td>Allows users to view and download the record of who has Viewed or Edited a Case that has been shared with them.</td>
</tr>
<tr>
<td>Citizen Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View Portals (Individual and Public)</td>
<td>No</td>
<td>—</td>
<td>Allows a user to view information about a portal, but not edit the information or view triage submissions.</td>
</tr>
<tr>
<td>Invite Individual</td>
<td>Yes</td>
<td>Citizen Management View Portals</td>
<td>Allows a user to create an individual portal for an individual citizen.</td>
</tr>
<tr>
<td>Create Public Portal</td>
<td>No</td>
<td>—</td>
<td>Allows a user to create a public portal that can be used by the community to upload items.</td>
</tr>
<tr>
<td>Edit and Close Public Portal</td>
<td>No</td>
<td>Citizen Management View Portals</td>
<td>Allows a user to edit and close (make inactive) a public portal. This can be set to allow the user to edit or close any portal or only the portals created by the user.</td>
</tr>
<tr>
<td>Triage Submissions</td>
<td>No</td>
<td>Evidence Management View Citizen Management View Portals</td>
<td>Allows a user to accept or decline items from individual invites and public portal submissions. This can be set to allow the user to triage submissions from any portal or only from portals created by the user. Requires: View Portals and View Evidence.</td>
</tr>
<tr>
<td>Audit Trail PDF</td>
<td>No</td>
<td>Citizen Management View Portals</td>
<td>Allows a user to view and download a PDF record of who has viewed, edited or triaged portals.</td>
</tr>
<tr>
<td>Email Notification Preferences</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account Lockout Notification</td>
<td>No</td>
<td>—</td>
<td>Determines whether or not a user receives Account Lockout Notifications when any user in the agency is locked out.</td>
</tr>
<tr>
<td>Upcoming Evidence Deletion Notification</td>
<td>No</td>
<td>—</td>
<td>Determines whether or not a user receives weekly notifications of any upcoming evidence deletions in the agency.</td>
</tr>
</tbody>
</table>
### Pre-Configured Roles and Default Permissions

The following table provides the default permissions for the pre-configured roles in Evidence.com. The settings for configurable roles can be changed by any user that has the Edit Agency Settings permission set to Allowed.

See the [Pre-Configured Lite Roles and Default Permissions](#) table for the permissions for pre-configured Lite roles.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Admin</th>
<th>User</th>
<th>Investigator</th>
<th>Armorer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Login Access</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evidence.com</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>Evidence Sync</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>Axon Capture</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Axon View XL</td>
<td>(as needed)</td>
<td>(as needed)</td>
<td>(as needed)</td>
<td>(as needed)</td>
</tr>
<tr>
<td><strong>User Account</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit Account Information</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>View &amp; Compose User Messages</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Download Sync Software</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>Create/Edit Group</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Group Audit Trail PDF</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td><strong>Admin Access</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure Agency Security Settings</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Edit Agency Settings</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Edit Device Offline &amp; Microphone Settings</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>CEW Administration</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Allowed</td>
</tr>
<tr>
<td>Device Administration</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Allowed</td>
</tr>
<tr>
<td>User Administration</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Allowed</td>
</tr>
<tr>
<td>Category Administration</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Allowed</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Generate Reports</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Allowed</td>
<td>Prohibited</td>
</tr>
<tr>
<td><strong>Search Access</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Search</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>Permission</td>
<td>Admin</td>
<td>User</td>
<td>Investigator</td>
<td>Armorer</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------</td>
<td>------------</td>
<td>--------------</td>
<td>---------</td>
</tr>
<tr>
<td>Partner Contact Search</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Evidence Search</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Device Search</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>Case Search</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
</tbody>
</table>

### Evidence Creation

<table>
<thead>
<tr>
<th>Permission</th>
<th>Admin</th>
<th>User</th>
<th>Investigator</th>
<th>Armorer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload External Files</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Configure Automatic Upload through Evidence Sync</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
</tbody>
</table>

### Evidence Management

<table>
<thead>
<tr>
<th>Permission</th>
<th>Admin</th>
<th>User</th>
<th>Investigator</th>
<th>Armorer</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Any Evidence</td>
<td>Only Their Own</td>
<td>Only Their Own</td>
<td>Prohibited</td>
</tr>
<tr>
<td>View CEW Firing Logs</td>
<td>Any Evidence</td>
<td>Only Their Own</td>
<td>Only Their Own</td>
<td>Only Their Own</td>
</tr>
<tr>
<td>Edit</td>
<td>Any Evidence</td>
<td>Only Their Own</td>
<td>Only Their Own</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Add/Remove Pending Review Category</td>
<td>Any Evidence</td>
<td>Only Their Own</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Redact</td>
<td>Any Evidence</td>
<td>Only Their Own</td>
<td>Only Their Own</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Order Transcript</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Reassign</td>
<td>Any Evidence</td>
<td>Only Their Own</td>
<td>Only Their Own</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Delete Evidence &amp; Edit Date Recorded</td>
<td>Any Evidence</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Download</td>
<td>Any Evidence</td>
<td>Only Their Own</td>
<td>Only Their Own</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Download Infected Files</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Share</td>
<td>Any Evidence</td>
<td>Only Their Own</td>
<td>Only Their Own</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Restrict</td>
<td>Any Evidence</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Share Externally to Authenticated Users</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Share External Download Links</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Post Notes</td>
<td>Any Evidence</td>
<td>Only Their Own</td>
<td>Only Their Own</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Audit Trail PDF</td>
<td>Any Evidence</td>
<td>Only Their Own</td>
<td>Only Their Own</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Access Restricted Evidence</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
</tbody>
</table>

### Case Management

<table>
<thead>
<tr>
<th>Permission</th>
<th>Admin</th>
<th>User</th>
<th>Investigator</th>
<th>Armorer</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Any Cases</td>
<td>Only Their Own</td>
<td>Any Case</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Permission</td>
<td>Admin</td>
<td>User</td>
<td>Investigator</td>
<td>Armorer</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------</td>
<td>----------------</td>
<td>---------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Edit</td>
<td>Any Cases</td>
<td>Only Their Own</td>
<td>Any Case</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Reassign</td>
<td>Any Cases</td>
<td>Only Their Own</td>
<td>Any Case</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Share</td>
<td>Any Cases</td>
<td>Only Their Own</td>
<td>Any Case</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Share with Partner Agencies</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Share External Download Links</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Audit Trail PDF</td>
<td>Any Cases</td>
<td>Only Their Own</td>
<td>Any Case</td>
<td>Prohibited</td>
</tr>
<tr>
<td>View &amp; Add Case Notes</td>
<td>Any Cases</td>
<td>Only Their Own</td>
<td>Any Case</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Create Case</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Restricted Category Access</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
</tbody>
</table>

**Shared Case**

<table>
<thead>
<tr>
<th>Permission</th>
<th>Admin</th>
<th>User</th>
<th>Investigator</th>
<th>Armorer</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>Edit</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>Reassign</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>Share</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>View &amp; Add Case Notes</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>Audit Trail PDF</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
</tbody>
</table>

**Citizen Management**

<table>
<thead>
<tr>
<th>Permission</th>
<th>Admin</th>
<th>User</th>
<th>Investigator</th>
<th>Armorer</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Portals (Individual and Public)</td>
<td>Any Portal</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Invite Individual</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Create Public Portal</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Edit and Close Public Portal</td>
<td>Any Portal</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Triage Submissions</td>
<td>Any Portal</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Audit Trail PDF</td>
<td>Any Portal</td>
<td>Prohibited</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
</tbody>
</table>

**Email Notification Preferences**

<table>
<thead>
<tr>
<th>Notification</th>
<th>Admin</th>
<th>User</th>
<th>Investigator</th>
<th>Armorer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Lockout Notification</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Allowed</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Upcoming Evidence Deletion</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Allowed</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Evidence Timestamp Notification</td>
<td>Allowed</td>
<td>Prohibited</td>
<td>Allowed</td>
<td>Prohibited</td>
</tr>
</tbody>
</table>

**Pre-Configured Lite Roles and Default Permissions**

The following table provides the default permissions for the preconfigured roles of Lite User and Lite Armorer. The Lite User and Lite Armorer roles are designed for users that only work...
with TASER Conducted Electrical Weapons (CEW) logs and TASER CAM videos. The Lite Armorer role acts as a CEW administrator and can reassign agency CEW devices, change CEW settings, and upload any CEW logs.

<table>
<thead>
<tr>
<th>Permission</th>
<th>Lite User</th>
<th>Lite Armorer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Login Access</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evidence.com</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>Evidence Sync</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>Axon Capture</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Axon View XL</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td><strong>User Account</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edit Account Information</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>View &amp; Compose User Messages</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>Download Sync Software</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>Create/Edit Group</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Group Audit Trail PDF</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td><strong>Admin Access</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure Agency Security Settings</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Edit Agency Settings</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Edit Device Offline &amp; Microphone Settings</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Device Administration</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>CEW Administration</td>
<td>Prohibited</td>
<td>Allowed</td>
</tr>
<tr>
<td>User Administration</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Category Administration</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Generate Reports</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td><strong>Search Access</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Search</td>
<td>Prohibited</td>
<td>Allowed</td>
</tr>
<tr>
<td>Partner Contact Search</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Evidence Search</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Device Search</td>
<td>Prohibited</td>
<td>Allowed</td>
</tr>
<tr>
<td>Case Search</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td><strong>Evidence Creation</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upload External Files</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Configure Automatic Upload through Evidence Sync</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td><strong>Evidence Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>View</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>View CEW Firing Logs</td>
<td>Only Their Own</td>
<td>Only Their Own</td>
</tr>
<tr>
<td>Edit</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Permission</td>
<td>Lite User</td>
<td>Lite Armorer</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------</td>
<td>--------------</td>
</tr>
<tr>
<td>Add/Remove Pending Review Category</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Redact</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Order Transcript</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Reassign</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Delete Evidence &amp; Edit Date Recorded</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Download</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Download Infected Files</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Share</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Restrict</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Share Externally to Authenticated Users</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Share External Download Links</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Post Notes</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Audit Trail PDF</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Access Restricted Evidence</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
</tbody>
</table>

**Case Management**

<table>
<thead>
<tr>
<th>Permission</th>
<th>Lite User</th>
<th>Lite Armorer</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Edit</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Reassign</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Share</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Share with Partner Agencies</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Share External Download Links</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Audit Trail PDF</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>View &amp; Add Case Notes</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Create Case</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Restricted Category Access</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
</tbody>
</table>

**Shared Case**

<table>
<thead>
<tr>
<th>Permission</th>
<th>Lite User</th>
<th>Lite Armorer</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Edit</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Order Transcript</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Reassign</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Redact</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Share</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>View &amp; Add Case Notes</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Audit Trail PDF</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
</tbody>
</table>

**Citizen Management**

<table>
<thead>
<tr>
<th>Permission</th>
<th>Lite User</th>
<th>Lite Armorer</th>
</tr>
</thead>
<tbody>
<tr>
<td>View Portals (Individual and Public)</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Invite Individual</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Permission</td>
<td>Lite User</td>
<td>Lite Armorer</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------</td>
<td>--------------</td>
</tr>
<tr>
<td>Create Public Portal</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Edit and Close Public Portal</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Triage Submissions</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Audit Trail PDF</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
</tbody>
</table>

**Email Notification Preferences**

<table>
<thead>
<tr>
<th>Email Notification Preferences</th>
<th>Lite User</th>
<th>Lite Armorer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Lockout Notification</td>
<td>Prohibited</td>
<td>Allowed</td>
</tr>
<tr>
<td>Upcoming Evidence Deletion Notification</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
<tr>
<td>Evidence Timestamp Notification</td>
<td>Prohibited</td>
<td>Prohibited</td>
</tr>
</tbody>
</table>
Appendix B: Traditional Media Player

Beginning with release 1.27, a new media player is the default player; however, users who want to use the traditional Evidence.com media player and redaction tools can switch to the traditional player and tools as needed.

For information about using the new media player, see Playing Video and Audio Evidence.

Working with Video and Audio Evidence

This section describes the actions available on the Evidence Detail page for video and audio files when you use the traditional media player.

Actions available for all file types are described in Working with Any Evidence.

Play, Pause, Rewind, and Fast Forward

On the Evidence Detail page, the video and audio player each provide the following basic functions:

- **Play** — Click anywhere on the player or, below the player, click (play).
- **Pause** — Click anywhere on the player or, below the player, click (pause).
- **Rewind** — Below the player, click . Each click rewinds the file approximately 4% of its overall length.
- **Fast Forward** — Below the player, click . Each click fast forwards the video approximately 4% of its total length.

Show and Hide Clock

In addition to the clock shown below the video image, you can show or hide the clock in the video image itself.

To show or hide the clock, on the toolbar, click .
**Magnify Zone**

You can use the zone magnification tool to zoom in on a portion of a video frame. You have the option of converting a magnified zone into a marker.

1. Play the video to about the frame that you want to magnify and then click [ ] (pause). You can pick the exact first frame more easily later.

2. From the tool bar, click [ ] (magnify zone).

   The zone magnification tool appears over the player.

   ![Magnify Zone Tool](image)

3. Use the zone magnification tool as needed to view details in the video.
   - To move the tool, at the top center of the tool, click and hold [ ] and then drag the tool to where you need.
   - To resize the tool, click and hold one of the corners ([ ] or [ ]) and then drag the corner until the tool is the size and shape that you need.
   - To skip backwards or forwards one second, click [ ] or [ ].
   - To expand what is inside the rectangle of the tool, at the bottom of the tool, click [ ].
   - To return to full frame from the expanded tool, at the bottom of the video image, click [ ].
   - To add or remove pixel smoothing, click [ ] or [ ].

4. If you want to save the magnified area as a marker, click [ ].

   The Add Marker dialog box appears. For more information, see Add Marker.
View Video Frame by Frame

1. Play the video to about the time that you want to view frame by frame and then click (pause).

2. From the tool bar, click (view frame by frame).

   Below the player, the frame-by-frame scrub bar appears. Each segment of the bar represents a video frame.

3. Use the frame-by-frame features as needed:
   - To preview frames, hover the mouse pointer over the scrub bar.
   - To go to a frame, click on its segment on the scrub bar.
   - To skip backwards or forwards one second, click or .

4. You can exit frame-by-frame viewing mode in one of two ways:
   - To remain at the last frame you viewed in frame-by-frame mode, click Continue.
   - To return to where you were in the video prior to viewing frame by frame, click Cancel.
Show and Hide Thumbnails

Thumbnails provide an easy way to preview parts of a video. They appear at the bottom of the video image. You can move the mouse pointer across them to see each thumbnail.

You can also control whether thumbnails appear.

- To hide thumbnails, click
- To show thumbnails, click

Rotate the Video

You can rotate the player image 90, 180, or 270 degrees clockwise. This feature is for convenience while viewing a video only. For example, the camera itself may have been on its side or upside down while recording.

The rotation does not affect the original video file and is not saved in any way. The next time you access the video, the video is not rotated.

To rotate the video image 90 degrees clockwise, click .
Markers

You can use markers to indicate key moments or highlight important aspects of a video or audio evidence file.

For video markers only, you can download markers as image files. Prior to downloading the marker, you can specify options such as whether the title and description appear on the downloaded image.

Show and Hide Markers

You can control whether the scrub bar, located below the video image, shows red icons for each marker.

- To hide marker icons on the scrub bar, click ✗ MARKERS.
- To show marker icons on the scrub bar, click MARKERS.

Add Marker

1. On the Evidence Detail page, below the player, click Add Marker.

   The Add Marker dialog box appears over the player.

2. Find the video frame that you want to mark.

   - To move rapidly through the video, on the scrub bar, click and hold  and then drag it left or right towards the frame that you want to mark.
   - To skip backwards or forwards one second, click  or .

3. In the Title box, type the title that you want to give the marker.

4. In the Description box, type a useful description of what is shown in the marker.

5. Select the marker options that you need.

   - To add fisheye distortion, click .
   - To use pixel smoothing, click .
   - To make the title, timecode, and description visible in the marker image, click .
6. Click **Add Marker**.

   The Add Marker dialog box closes.

   The new marker icon appears on the scrub bar at the time where you added the marker.

   Below the player, under Markers, the new marker appears in the list of markers.

---

**Edit Marker**

1. On the Evidence Detail page, below the player and under Markers, find the marker that you want to edit.

2. Click the marker name.

   The player jumps to the marker. In a transparent dialog box over the player, the name and timecode of the marker appear.

3. In the transparent dialog box, click **Edit**.

   The Edit Marker dialog box appears.

4. If you want to change the video frame of the marker, find the video frame that you want to mark.

   - To move rapidly through the video, on the scrub bar, click and hold ‹ and then drag it left or right towards the frame that you want to mark.

   - To skip backwards or forwards one second, click ‹‹ or ‹›.

5. If you want to edit the title, in the **Title** box, type the new title that you want to give the marker.

6. If you want to edit the description, in the **Description** box, type a new, useful description of what is shown in the marker.

7. Select the marker options that you need.

   - To add fisheye distortion, click †

   - To use pixel smoothing, click ‡

   - To make the title, timecode, and description visible in the marker image, click ‡

8. Click **Edit Marker**.

   The Add Marker dialog box closes.
The new marker icon appears on the scrub bar at the time where you added the marker.

Below the player, under Markers, the new marker appears in the list of markers.

**View Marker**

1. On the Evidence Detail page, below the player and under Markers, find the marker that you want to view.

2. Click the marker name.

   The player jumps to the marker. The name and timecode of the marker appear over the bottom of the video.

**Download Marker**

You can download a video marker as a PNG file.

1. On the Evidence Detail page, below the player and under Markers, find the marker that you want to download.

2. To the left of the marker, click ‌(download).

   The Download Marker dialog box appears.

3. If you want to modify the title or description or if you want to select marker options, you can do so prior to downloading the marker.

   For more information, see Edit Marker.

4. Click **Download Marker**.

5. Use the dialog box that appears to save the marker to your computer.

6. On the Download Marker dialog box, in the upper-left corner, click ‌(exit).

**Delete Marker**

1. On the Evidence Detail page, below the player and under Markers, find the marker that you want to delete.

2. Click the marker name.

   The player jumps to the marker. In a transparent dialog box over the player, the name and timecode of the marker appear.
3. In the transparent dialog box, click **Delete** and then click **Confirm**.

The deleted marker no longer appears in the Markers list below the player.

---

** Clips **

A clip is a segment of a video or audio evidence file. When you create a clip, Evidence.com creates a new evidence file that you can use in the same way as other evidence.

** Show and Hide Clips **

You can control whether the scrub bar, located below the video image, shows yellow zones for each clip.

- To hide clip zones on the scrub bar, click ![Hide Clips](clips.png)
- To show clip zones on the scrub bar, click ![Show Clips](clips.png)

** Add Clip **

1. On the Evidence Detail page, below the video or audio player, click **Add Clip**.

The Create Clip dialog box appears over the player. On the scrub bar, two blue sliders appear. The time to the left of the scrub bar is the start time of the clip. The time to the right of the scrub bar is the end time of the clip.
2. Use the two blue sliders to set the start and end of the clip.
   - To set the start of the clip, click and hold the left slider and then drag it to the time where you want the clip to start.
   - To set the end of the clip, click and hold the right slider and then drag it to the time where you want the clip to end.

3. On the video or audio player window, click ▶ (play) and review the clip.

4. If necessary, repeat steps 2 and 3 until the start and end of the clip are what you need.

5. In the Title box, type the title that you want to give the clip.

6. In the Description box, type a useful description of what is shown in the clip.

7. Click Create Clip.

8. On the notification message box, click OK.

   Evidence.com generates a new video title, “Clip from [original evidence title]”. You can use an evidence search to find the video or audio clip.

**View Clip**

You can access clips from the Evidence Detail page of the evidence from which the clip was made.

1. On the Evidence Detail page, below the video or audio player and under Clips, find the clip that you want to view.

2. Click the clip title.

   The Evidence Detail page for the clip opens.

3. Use the features of the Evidence Detail page as needed.

**Redacting a Single Video**

For information about using the new redaction tools, see Video Evidence Redaction.

You can redact video evidence as needed, such as to ensure anonymity of persons in a video. Redaction never affects the original video. Instead, when you have finished redacting the video, Evidence.com generates a redacted version of the video.
The process of redaction involves placing one or more masks in the video. You can specify precisely which video frame a redaction mask applies to. The redaction mask types are the following:

- **Vector** — Redacts a portion of video frames, in a shape, color, and opacity that you specify.
- **Blackout mask** — Replaces video frames with a solid black frame.
- **Filter mask** — Obscures entire video frames with either a blur filter, an outline distortion filter, or a segmentation filter.
- **Audio mask** — Remove the audio from the frames that you apply the mask to.

For the video masks, you have the option of also redacting audio for the duration of the mask.

1. Play the video to about the first frame that you want to apply a new mask to and then click \( \text{pause} \). You can pick the exact first frame more easily later.

2. From the tool bar, click \( \text{redact video} \).
   The Redaction Masks dialog box appears over the player.

3. Apply redaction masks to the video as needed. You can apply as many masks as required to ensure that the video is redacted to suit your needs. For information about specific mask types, see the following topics:
   - Add a Vector Mask
   - Add a Blackout Mask
   - Add a Filter Mask
   - Add an Audio Mask

4. Modify masks as needed. For information about specific actions, see the following topics:
   - Editing a Mask
   - Preview Mask
   - Rename a Mask
   - Deleting a Mask

5. On the Redaction Masks dialog box, click **Finish**.
On the notification message box, click **OK**.

Evidence.com generates a new video title, “Redacted video of [original video title]”. You can use an evidence search to find the redacted video.

### Add a Vector Mask

You can use a vector mask to redact parts of individual video frames. You can also redact the audio associated with those frames.

1. If the Redaction Masks dialog box is not open, from the tool bar on the player, click **(redact video)**.

   The Redaction Masks dialog box appears over the player.

2. Click **New Mask**.

   The Add Mask dialog box appears.

3. Under **Mask Style**, click **Vector Mask**.

4. Under **Duration**, click **Find**.

   The Find First Frame Viewer shows the current frame.

5. Move the slider until the first frame that you want to redact appears.

6. Click **Confirm**.

   The Add Mask dialog box reappears.

7. Under **Color**, click **View**.

   The Opacity and Color Viewer shows a preview of the current frame and the selected vector details.

   By default, the mask is black and opaque (100% opacity).

8. If you want to change the mask color, click the desired color.

9. If you want the vector mask to be transparent, move the **Opacity** slider until the mask shown in the frame thumbnail under Mask Style.

10. Click **Confirm**.

    The Add Mask dialog box reappears.
11. Under Vectors, select the shape of the vector mask:
   - Elliptical
   - Rectangular

12. Choose whether you want to redact the area inside or the area outside of the vector mask:
   - Interior — Redact what is inside of the vector mask.
   - Inverted — Redact what is outside the vector mask.

13. Under Audio, select whether the audio associated with the redacted frames will be redacted, too. By default, audio is redacted. If you do not want to redact the audio, clear the “Redact associated audio” check box.

14. Click Continue.

   The video frame that you selected appears with the vector mask over it. Below the video is a frame bar that enables you to select other frames.

15. Apply the vector mask to frames as needed. The following table lists basic actions for applying a mask.

<table>
<thead>
<tr>
<th>Basic Action</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select a frame</td>
<td>You can do any of the following:</td>
</tr>
<tr>
<td></td>
<td>- To move forward one frame, press Right Arrow or D.</td>
</tr>
<tr>
<td></td>
<td>- To move backward one frame, press Left Arrow or A.</td>
</tr>
<tr>
<td></td>
<td>- To jump to a specific frame, move the mouse pointer over</td>
</tr>
<tr>
<td></td>
<td>the frame bar to the desired frame and click it.</td>
</tr>
<tr>
<td>Move the mask</td>
<td>1. Click and hold the mask, avoiding the handles at the</td>
</tr>
<tr>
<td></td>
<td>corners.</td>
</tr>
<tr>
<td></td>
<td>2. Drag the mask to where you want it.</td>
</tr>
<tr>
<td></td>
<td>3. Release the mouse button.</td>
</tr>
<tr>
<td>Shape the mask</td>
<td>1. Click and hold a handle at one corner of the mask.</td>
</tr>
<tr>
<td></td>
<td>2. Drag the corner to where you want it.</td>
</tr>
<tr>
<td></td>
<td>3. Release the mouse button.</td>
</tr>
<tr>
<td>Apply the mask to the frame</td>
<td>Press Down Arrow or S.</td>
</tr>
<tr>
<td>Clear the mask from a frame</td>
<td>Press Up Arrow or W.</td>
</tr>
</tbody>
</table>
You can also use the following advanced actions.

<table>
<thead>
<tr>
<th>Advanced Action</th>
<th>Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Go to the next segment of video</td>
<td>Press Shift + Right Arrow or press Shift + D.</td>
</tr>
<tr>
<td>Go to the previous segment of video</td>
<td>Press Shift + Left Arrow or press Shift + A.</td>
</tr>
</tbody>
</table>
| Apply the mask to a range of frames | If you do not need to move the mask from frame to frame, you can apply it to the range of frames:  
1. Select the first frame in the range.  
2. Apply the mask to the first frame.  
3. Select the last frame in the range.  
4. Apply the mask to the last frame.  
After you finish applying the mask, Evidence.com adds the mask to all frames in the range. |

16. After you have applied to mask to the frames you want to redact, click **Confirm**.

The Redaction Masks dialog box lists the vector mask that you created.

**Add a Blackout Mask**

1. If the Redaction Masks dialog box is not open, from the tool bar on the player, click **(redact video)**.  
The Redaction Masks dialog box appears over the player.

2. Click **New Mask**.  
The Add Mask dialog box appears.

3. Under **Mask Style**, click **Blackout Mask**.

4. Under **Duration**, next to **Start Time**, click **Find**.  
The Find First Frame Viewer shows the current frame.

5. Move the slider until the first frame that you want to redact appears.

6. Click **Confirm**.  
The Add Mask dialog box reappears.

7. Under **Duration**, next to **End Time**, click **Find**.  
The Find Last Frame Viewer shows the current frame.

8. Move the slider until the last frame that you want to redact appears.
9. Click Confirm.

The Add Mask dialog box reappears.

10. If you want to change the mask color, under Color, click the desired color.

11. Under Audio, select whether the audio associated with the redacted frames will be redacted, too. By default, audio is redacted. If you do not want to redact the audio, clear the “Redact associated audio” check box.

12. Click Confirm.

The Redaction Masks dialog box lists the vector mask that you created.

Add a Filter Mask

1. If the Redaction Masks dialog box is not open, from the tool bar on the player, click (redact video).

The Redaction Masks dialog box appears over the player.

2. Click New Mask.

The Add Mask dialog box appears.

3. Under Mask Style, click Filter Mask.

4. Under Duration, next to Start Time, click Find.

The Find First Frame Viewer shows the current frame.

5. Move the slider until the first frame that you want to redact appears.

6. Click Confirm.

The Add Mask dialog box reappears.

7. Under Duration, next to End Time, click Find.

The Find Last Frame Viewer shows the current frame.

8. Move the slider until the last frame that you want to redact appears.

9. Click Confirm.

The Add Mask dialog box reappears.
10. Under **Filter Effect**, click the desired filter.
   - Blur
   - Outline Distortion
   - Segmentation
   
   To see an example of each filter type, hover the mouse pointer over the filter name.

11. Under **Audio**, select whether the audio associated with the redacted frames will be redacted, too. By default, audio is redacted. If you do not want to redact the audio, clear the “Redact associated audio” check box.

12. Click **Confirm**.

   The Redaction Masks dialog box lists the vector mask that you created.

---

### Add an Audio Mask

1. If the Redaction Masks dialog box is not open, from the tool bar on the player, click ![redact video](redact video). The Redaction Masks dialog box appears over the player.

2. Click **New Mask**.

   The Add Mask dialog box appears.

3. Under **Mask Style**, click **Audio Only**.

4. Under **Duration**, next to **Start Time**, click **Find**.

   The Find First Frame Viewer shows the current frame.

5. Move the slider until the first frame that you want to redact appears.

6. Click **Confirm**.

   The Add Mask dialog box reappears.

7. Under **Duration**, next to **End Time**, click **Find**.

   The Find Last Frame Viewer shows the current frame.

8. Move the slider until the last frame that you want to redact appears.

9. Click **Confirm**.
The Add Mask dialog box reappears.

10. Click **Confirm**.

The Redaction Masks dialog box lists the vector mask that you created.

### Editing a Mask

1. If the Redaction Masks dialog box is not open, from the tool bar on the player, click (redact video).

   Over the player, the Redaction Masks dialog box lists all the masks.

2. To the right of the mask that you want to edit, click **Edit**.

   The Edit Mask dialog box appears.

3. Change the mask as needed. For more information about options available for each type of mask, refer to the topic for adding that mask type:
   - Add a Vector Mask
   - Add a Blackout Mask
   - Add a Filter Mask
   - Add an Audio Mask

### Preview Masks

1. If the Redaction Masks dialog box is not open, from the tool bar on the player, click (redact video).

   Over the player, the Redaction Masks dialog box lists all the masks.

2. Choose how you want to preview masks:
   - If you want to preview a single mask, next to the mask name, click **Preview**.
   - If you want to preview all masks, click **Preview All**.

   The player shows you the portions of the video affected the mask you selected or by all masks.
3. To end the preview, click || (pause).

After you end the preview or after the preview completes, the Redaction Masks dialog box appears again.

**Rename a Mask**

1. If the Redaction Masks dialog box is not open, from the tool bar on the player, click  (redact video).

   Over the player, the Redaction Masks dialog box lists all the masks.

2. Click the name of the mask that you want to rename.

3. In the **Mask Name** box, type the new name for the mask, and then click **OK**.

**Deleting a Mask**

1. If the Redaction Masks dialog box is not open, from the tool bar on the player, click  (redact video).

   Over the player, the Redaction Masks dialog box lists all the masks.

2. For each mask that you want to delete, click × (delete) and then click **Confirm**.

   The deleted masks no longer appear on the Redaction Masks dialog box.
Appendix C: Body Camera and Fleet Camera Settings

This appendix provides descriptions and additional information for each of the settings on the Body Camera Settings page and Fleet Settings page.

Body Camera Settings

This section provides additional details for each of the settings on the Body camera settings page.

Axon Body and Axon Flex Camera Settings

Video Settings

• Pre-Event Buffering

This setting determines if video in the pre-event buffer is included in a video recording. When enabled, video from the 30 seconds prior to the user starting a camera recording is included in the final video.

• Quality Settings

This sets the video quality for body camera recordings. Higher quality videos will take up more storage space. For the best balance of quality and storage space, Axon recommends that the cameras record in Medium.

Audio Recording Settings

• Camera Audio Recording

This sets if the camera records audio while recording video.

Axon Body 2 and Axon Flex 2 Camera Settings

Video Settings

• Quality Settings

This sets the video quality for body camera recordings. Higher quality videos will take up more storage space. For the best balance of quality and storage space, Axon recommends that the cameras record in Low HD.

Note: If the Quality Setting High HD (1080P) is selected, the Pre-Event Buffering setting cannot be set to 120 seconds.
• **Pre-Event Buffering**

  This setting determines if video in the pre-event buffer is included in a video recording. The pre-event buffering time is configurable in 30 second increments for up to 120 seconds (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.

  **Note:** Pre-event buffering settings above 30 seconds are only available for Axon Body 2 and Axon Flex 2 cameras with the v1.9 firmware release or higher. Additionally, pre-event buffering cannot be set to 120 seconds if the Quality Setting is High HD (1080P).

• **Watermark**

  This setting controls if a permanent watermark appears in the upper right corner of all Axon Body 2 and Axon Flex 2 camera videos. The watermark displays the date, time, and camera serial number for the duration of the video.

  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.

  **Why does the Watermark use UTC time?**

  UTC is based on Greenwich Mean Time (GMT) however the use of UTC is preferred because Greenwich observes daylight savings time in the form of British Summer Time (BST), then switches back to GMT in the winter.

  The International Organization for Standardization (ISO) created the Coordinated Universal Time (UTC) as a way to represent dates and times using numbers in a form that is accepted by the national standardization body in most countries globally. This standard is used by most militaries and the aviation industry worldwide to ensures that all references to time are coordinated to the same standard.

  Axon believes it is critical to maintain the UTC time standard for all videos and therefore cannot support customization of the watermark to match a particular customers local time zone.

  After uploading, Evidence.com converts the time for each video to local time shown in the upper right corner next to the video player.

• **Show Recording Status with Front Camera Light**

  This setting enables the visible indication of the recording status on the front of the camera using the battery LED. During pre-event buffering the light will blink green.
During recording the light will blink red. If the front camera light is enabled, users can turn it off by turning off all indicator lights or by entering Stealth Mode.

**Audio Settings**

- **Camera Audio Recording**
  
  This sets if the camera records audio while recording video.

  To mute the audio on all Axon Body 2 and Axon Flex 2 camera videos at your agency, select **Disable Camera Audio Recording**. If you do not want users to have the ability to turn audio recording for their camera back on, then the **Toggle Camera Audio Recording** setting must be set to Prohibit Users from Toggling Camera Audio.

- **Toggle Camera Audio Recording**

  This setting controls if users can enable and disable audio while recording an event.

  Audio is muted during a recording by pressing and holding the function button for 3 seconds.

- **Pre-Event Buffering Audio Recording**

  This setting determines if audio will be recorded in the pre-event buffer.

**Connectivity Settings**

Note: Visibility of the Bluetooth setting is managed by an Axon-controlled agency level setting. Agencies that would like to have the Bluetooth setting available can contact their Axon representative or Technical Support to request this option.

- **Bluetooth**

  This setting controls the camera's ability to use Bluetooth features. Disabling this setting turns off Bluetooth for all Axon Body 2 and Axon Flex 2 cameras at your agency. Bluetooth features including Axon Signal, Axon View, and Multicam will be disabled.

**Application Support Settings**

- **Axon View Pairing**

  This sets if the cameras can be paired with the Axon View mobile application.
• **Axon View Login**

   Enabling this setting forces users to log in to Axon View before they can pair with Axon cameras. Note: If your agency has IP restrictions enabled, all mobile devices must have VPN access to your network.

**Axon Signal Settings**

• **Axon Signal**

   This setting controls the camera's ability to activate recording when alerted by Axon Signal products. The trigger events for the cameras are set on the Signal Configuration page.

**User Configurable Settings**

• **User Configurable Modes: Stealth and Indicator Lights**

   This setting allows camera users to turn on or off (toggle) stealth mode or indicator lights. Axon Body 2 and Axon 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. When officers enable stealth mode, all lights, sounds, and vibrations are turned off. When officers disable indicator lights, all lights are turned off. These settings will also disable the front camera light regardless of the **Show Recording Status with Front Camera Light** setting.

**Additional Settings**

• **Bookmark while Recording**

   This setting controls if users can leave a bookmark on a video while the camera is recording. Bookmarks are added to the recording by pressing the function button on the side of the camera. This function can be used to quickly note the time of a memorable incident while the camera is recording. The bookmark will be visible when viewing the video on Evidence.com.

**All Body Camera Settings**

• **Offline Configuration**

   This sets if Axon Body2, Axon Body, Axon Flex 2, and Axon Flex cameras can be set to and used in standalone (or offline) mode. Selecting the checkbox below enables individual devices to be set to offline mode using the Evidence Sync application.
**WARNING:** Enabling offline mode requires users to accept a disclaimer acknowledging risks to the agency and data when configuring Axon video devices in offline mode.

## Fleet Settings

This section provides additional details for each of the settings on the Fleet settings page. The front camera light and quality settings can be set separately for the Fleet Front and Back cameras. When View XL is connected to Evidence.com, it automatically checks for and applies any updated Axon Fleet configuration settings every 10 minutes.

### Video Settings

- **Pre-Event Buffering**
  
  This setting determines if video will be recorded in the pre-event buffer.

- **Show recording status with front camera light**
  
  This setting enables the visible indication of the recording status on the front of the camera using the battery led. During pre-event buffering the light will blink green. During recording the light will blink red.

- **Quality settings**
  
  This sets the video quality that Fleet cameras will record in. Each Fleet camera can have a different setting. Higher quality videos will take up more storage space. For the best balance of quality and storage space, Axon recommends that the cameras record in low HD.

- **User Configurable Modes: Stealth and Indicator Lights**
  
  This setting allows Fleet camera users to turn on or off (toggle) stealth mode or indicator lights. 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**
  
  This setting controls whether or not a permanent watermark appears in the upper right corner of all Fleet videos. The watermark displays the date, time, and camera serial number for the duration of the video.
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.

**Why does the Watermark use UTC time?**

UTC is based on Greenwich Mean Time (GMT) however the use of UTC is preferred because Greenwich observes daylight savings time in the form of British Summer Time (BST), then switches back to GMT in the winter.

The International Organization for Standardization (ISO) created the Coordinated Universal Time (UTC) as a way to represent dates and times using numbers in a form that is accepted by the national standardization body in most countries globally. This standard is used by most militaries and the aviation industry worldwide to ensure that all references to time are coordinated to the same standard.

Axon believes it is critical to maintain the UTC time standard for all videos and therefore cannot support customization of the watermark to match a particular customer’s local time zone.

After uploading, Evidence.com converts the time for each video to local time shown in the upper right corner next to the video player.

### Audio Settings

- **Camera Audio Recording**

  This sets if the Fleet cameras, Front and Back, will record audio while recording video. To prevent Fleet cameras from recording audio, select **Disable Camera Audio Recording**.

- **Toggle Camera Audio Recording**

  This setting controls if your users can use View XL to enable or disable audio recording while the Fleet cameras are recording video. This setting is only applicable if the Camera Audio Recording setting is set to **Enable Camera Audio Recording**. When **Allow Users to Toggle Camera Audio** is selected, additional audio controls are available to the users in View XL. If you do not want your users to be able to mute audio recording, select **Prohibit Users from Toggling Camera Audio**.

- **Pre-event buffering audio recording**

  This setting determines if audio will be recorded in the pre-event buffer.
Activation Settings

- **Speed Activation**
  
  **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.

  This setting allows you to configure your Axon Fleet Front camera to transition from Buffering to Event mode to record video when the set speed threshold is exceeded. Use the **Speed Activation** slider to set the speed. Speed activation is off by default.

- **Acceleration Activation**

  This setting enables Fleet cameras to transition from Buffering to Event mode when sensors detect very high sudden changes in acceleration, usually associated with vehicle accidents or crashes. This setting is disabled by default.

Offload Settings

- **Auto Offload Timer**

  This sets the amount of time that evidence is stored in View XL before being automatically queued for upload to Evidence.com. It can be configured for immediate queuing or with a delay of 1 to 12 hours, set in one-hour increments.
## Revision History

This section summarizes the changes to this guide, per each version of the guide. The revision table lists the versions in reverse order, so that you can more easily see the most recent changes to the guide.

<table>
<thead>
<tr>
<th>Release Name and Document Revision</th>
<th>Revision description</th>
</tr>
</thead>
</table>
| October 2018 Rev A                 | • Updated Axon Citizen – Citizen Evidence and Portal Details Page Overview section with information about Owner column and filters.  
• Updated the Evidence Search Filters – Advanced Search Filters section with information on the new Source filter.  
• Added the procedure for Axon Fleet Bulk Vehicle Creation to the Vehicle search section.  
• Updated the Early Access Devices section to include Axon Flex 2 cameras and controllers as early access devices.  
• Updated descriptions of special categories with the following changes – the Uncategorized category can have an evidence retention policy setting and Pending Review can be a restricted category. |
| September 2018 Rev A               | • Updated Axon Citizen Portal Details pages section with information about links to the Evidence Search pages and the Portal Owner field.  
• Updated the Creating a Public Portal procedure with the Portal Owner field information. Added procedures for editing and closing a Public Portal.  
• Updated the Additional Information on the Citizen Evidence Detail Pages section with the Triaged By field information.  
• Updated the Redaction Studio description and images to include segment timelines.  
• Updated the Body Camera Settings section with the reorganized settings and descriptions. |
| August 2018 Rev A                  | • Added information about and procedures for using Axon Citizen for Communities. Including permissions, creating public portals, and what community members see.  
• Added information on new Redaction Studio keyboard controls for changing playback speed and adding audio masks.  
• Updated Inventory Page section for changes to main page.  
• Added new In Evidence device status description.  
• Updated Citizen Settings for Axon Citizen for Communities.  
• Updated Appendix A Citizen Management Permissions.  
• Added information to Appendix C Fleet Settings about new Axon Fleet Auto Offload Timer setting. |
<table>
<thead>
<tr>
<th>Release Name and Document Revision</th>
<th>Revision description</th>
</tr>
</thead>
</table>
| July 2018 Rev A                    | • Added information about the new Inventory pages, which replaces Devices page, and moved information for Axon Fleet Vehicles to this section.  
• Updated the Add, Edit and Delete a Retention Category information for user interface changes.  
• Added note to the Axon Citizen Instructions for Evidence collectors section saying that for agencies that have French set as default language, the Axon Citizen individual invite text, Terms of Use, and Privacy Policy information will also appear in French. Updated the maximum submission file size to 60 GB.  
• Updated contact email for Axon Technical Support to support@axon.com. |
| June 2018 Rev A                    | • Updated file size information limits Axon Citizen submissions.  
• Updated the Using Evidence.com to Triage Submissions section with information on the Accept and Decline Remaining buttons.  
• Updated the Redaction Studio section with information on the playback speed selector control.  
• Updated Evidence Edit Location procedure with information about using latitude and longitude coordinates.  
• Updated the Admin - Citizen Settings section for changes to setting text and order.  
• Added the Download Evidence Upload XT section.  
• Added the **User Configurable Modes: Stealth and Indicator Lights** setting to Axon Fleet Settings descriptions. |
| May 2018 Rev A                     | • Removed Grant Temporary Access to Customer Service section – This option was removed to update the functionality.  
• Updated Axon Citizen section with new information about the triage workflow, permissions, Axon Citizen settings, virus scan, and what community members see.  
• Added new keyboard controls for Redaction Studio.  
• Updated the Citizen Settings section with new triage workflow setting information.  
• Updated Appendix A Roles and Permissions for new Citizen Management and Download Infected Files permissions. |
| April 2018, Rev A                  | • Updated the Update Your Email Notifications procedure to reflect the updated Email Notifications page.  
• Added a note to the Evidence, Cases, and Devices Export Search Results sections saying when search results are exported in Microsoft Excel or CSV format, the Device Assignee First Name and Last Name are split into separate columns and a Badge ID column is included.  
• Added a section for the new Field Validation Admin page and incorporated the existing information on using Regex.  
• Added a note to the Groups Administration User Permission section and set-up procedures saying that when License Tiers are enforced or in preview mode for an agency, Group Monitors must be assigned to a Pro Tier role.  
• Updated the Add Category, Edit Category, and Delete Category procedures for changes due to Field Validation.  
• Updated the Configure CEW Signal Settings procedure with information about Assigned Officer Activation setting.  
• Updated the description for the Edit Agency Settings permission to show it is used to access the Field Validation page. |
<table>
<thead>
<tr>
<th>Release Name and Document Revision</th>
<th>Revision description</th>
</tr>
</thead>
</table>
| March 2018 Rev A                  | Added information in the Sign In to Evidence.com section about how users can search for their agency's Evidence.com site.  
Updated Outside My Agency evidence access list procedures (Adding Users and Groups to an Outside My Agency Access List from the Evidence Search Page, Adding Users and Groups to the Outside My Agency Access List, and Modifying and Removing Users and Groups from Outside My Agency Access Lists) to include information about Partner Agency Groups.  
Added information about the Most Recent Dock Connection to the Summary tab description in View Device Profile.  
Added information to the Evidence Created and Evidence Deleted report descriptions about showing the difference between evidence recording and evidence upload. |
| February 2018 Rev A               | Added Axon Citizen section for users.  
Updated Text Search Details section for Evidence Search Filters and Case Search Filters.  
Updated evidence access list procedures with the group changes.  
Updated Evidence Map and Cases View Map sections with the updated map information.  
Added Redaction Studio section.  
Updated Group Administration section with information for Groups changes.  
Added Citizen Settings section for administrators.  
Updated Categories and Evidence Retention Policies section to remove information about map pins.  
Updated Configure CEW Settings section with information about new Continued SPPM Transmit in Safe Setting.  
Updated Appendix A with new Citizen Management permission. |
| January 2018 Rev A                | Reorganized guide content, placing information on evidence management, case management, device management, and reporting in the front portion of the guide. Administrator-only information was moved to be later in the guide. Renamed the guide as Evidence.com User and Administrator Reference Guide.  
Corrected the About the Access Restricted Evidence Permission section, which had out-of-date information.  
Removed the reference to editing time zone in the Edit Other User Account Information section. |
| December 2017 Rev A               | Updated the Configure Password Settings section to include information about the configurable Session Timeout setting.  
Added a note to the Export Device Search Results section that says the Device Assignee First Name and Last Name are split into separate columns when Device Search results are exported in Microsoft Excel or CSV format.  
Corrected some descriptions and default permissions in Appendix A. |
<table>
<thead>
<tr>
<th>Release Name and Document Revision</th>
<th>Revision description</th>
</tr>
</thead>
</table>
| October 2017 Rev A                | • Added that users can enter their username or email address in the Username field when signing in to Evidence.com.  
• Added a note to the Regular Expressions for Evidence ID Validation section saying that the current version of Evidence Synch does not support Regular Expressions with `/i`. Support for this will be added in a future Evidence Synch release.  
• Updated Signal Configuration section with information on settings for Signal Sidearm.  
• Added Signal Sidearm Registration section with information on registering Signal Sidearm devices.  
• Added a note to the Restore Evidence and Restore Deleted Evidence sections saying that when evidence that is queued for deletion is restored, if the evidence is assigned a category that has a retention period, the evidence's new deletion date is set 30 days from the current date, regardless of the categories retention period.  
If the evidence is uncategorized or the assigned category does not have a retention period, then no deletion date is set for the evidence.  
• Added information to the Assign and Un-Assign Categories section saying that the Categories area appears in the heading below the evidence Title and ID and on the right side of the page. Updated procedure for assigning categories for other UX updates.  
• Added notes to the Appendix C Body Camera Settings descriptions for Axon Body2 and Axon Flex 2 Cameras saying the setting combination of Video Quality High HD (1080P) and Pre-Event Buffering 120 seconds is not allowed. |
| September 2017 Rev A              | • Added Device Serial to the list of Advanced Search filters.  
• Added procedures for using Inside My Agency access lists and updated procedures for Outside My Agency access lists to replace the previous sharing procedures.  
• Updated the description of the User Summary Report to include Last Login Date, Invited Date, and Deactivated Date.  
• Renamed the Evidence Management Restricted Category Access permission to Access Restricted Evidence and updated the permission description in Appendix A: Roles and Permissions. |
| August 2017 Rev A                 | • Updated the Evidence Search Filters Date filter to include time information.  
• Added a note about the transition from the current evidence sharing workflow to the new Evidence Access List functionality in the Bulk Share Evidence by Authenticated Sharing, Bulk Share Evidence by Unauthenticated Download Link, and Share an Evidence File sections.  
• Corrected the name and description for Activation Settings in the Fleet Settings section of Appendix C. |
| July 2017 Rev A                   | • Removed Internet Explorer 10 from the list of supported browsers.  
• Clarified the note in the Multicam Playback – Selecting Videos for Playback section to say that cameras must be within range of each other for at least one minute before recording, excluding pre-event buffering, for the videos to be displayed with multicam playback.  
• Updated the Fleet Settings section of Appendix C with new Audio Settings and Activation Settings for Fleet cameras. |
<table>
<thead>
<tr>
<th>Release Name and Document Revision</th>
<th>Revision description</th>
</tr>
</thead>
</table>
| June 2017 Rev A                    | • Added and updated information and procedures to support Axon Fleet in Evidence.com, this includes Axon Fleet camera settings, Vehicle configuration, and Signal configuration.  
                              | • Updated the Multi-Factor Authentication Security Challenge Frequency maximum setting to 20 minutes.  
                              | • Added information on Evidence Search - User Association and Vehicle ID Advanced Search filters.  
                              | • Added note to the Multicam Playback – Selecting Videos for Playback section saying that videos must be at least one minute in length, excluding pre-event buffering, to be displayed with multicam playback.  
                              | • Added information on Device Summary Report to the Reporting section.  
                              | • Updated Appendix C to include information on Axon Fleet camera settings. |
| May 2017 Rev A                     | • Added Multi-Factor Authentication section (this replaces the Mobile Phone Advanced Authentication section)  
                              | • Updated Supported File Types section by adding .wma as a supported audio file type. Note that Evidence.com already supported .wma file types, but the list in the guide did not reflect this. |
| April 2017 Rev A                   | • Updated the Supported Web Browsers section with a note saying that Evidence.com will no longer support Internet Explorer 10 beginning with the July 2017 release of Evidence.com.  
                              | • Updated the Complete the User Registration Process section by removing the reference to accepting the End User License Agreement (EULA). |
| March 2017 Rev B                   | • Updated company name information. |
| March 2017 Rev A                   | • Added a procedure to Copy a Role.  
                              | • Added information and procedures for Early Access Devices.  
                              | • Updated the Video Evidence Redaction section and added information about Skin Blur Redaction.  
                              | • Added Appendix C: Body Camera Settings with descriptions of the Evidence.com settings for Axon Body 2, Axon Flex 2, Axon Body, and Axon Flex cameras. |
| February 2017 Rev A                | • Updated the Roles and Permissions section with new pre-configured role information, the new license Tier setting for roles, and updated Appendix A: Roles and Permissions with new role and permission setting information. Removed the section on Assignee Only role, since this role is no longer available.  
                              | • Added a note to the Configure Password Settings section with information about failed security question attempts.  
                              | • Updated the Evidence Search section for changes to the Evidence.com search functions.  
                              | • Added a section on download speed information.  
                              | • Updated the Edit Location topic to say the location area appears in the upper-right.  
<pre><code>                          | • Added information about the Multicam Playback feature. |
</code></pre>
<table>
<thead>
<tr>
<th>Release Name and Document Revision</th>
<th>Revision description</th>
</tr>
</thead>
</table>
| January 2017 Rev A                | • Added Microsoft Edge to the list of supported web browsers.  
• Added a note for Internet Explorer 11 users saying that Font downloads must be enabled to use Evidence.com.  
• Added a note about the temporary file size limit for Bulk Download Evidence.  
• Added information about Audit Trail information for all devices. |
| December 2016 Rev. A              | • Added information about the Evidence.com on-demand transcription service and procedures for:  
  o Transcription Service Setup  
  o Requesting Transcriptions  
• Added information about new  
• Added information about the Audit Trail Information for Axon Body 2 and Flex 2 cameras. |
| October 2016 Rev. A               | • Added the Configure Signal Settings section, which includes settings for Axon Signal Unit and CEWs.  
• Updated the following two sections, in support of changes to redaction workflows:  
  o Extract a Redacted Video from a Redaction  
  o View Evidence Extracted from Clips, Markers, and Redactions  
• Added the Upload a Third-Party Redacted Video section. |
| September 2016                    | No changes were made to this guide in support of Evidence.com September 2016. |
| August 2016                       | No changes were made to this guide in support of Evidence.com August 2016. |
| July 2016 Rev. A                  | Mask sizes for manual redactions enables agencies to more precisely redact small objects. |
| June 2016 Rev. A                  | • Axon Body 2 camera enhancements — Administrators can allow officers to enable/disable the indicator lights on their cameras.  
• CEW device setting update — The APPM setting now also controls the new Signal Performance Power Magazines (SPPMs).  
• Redaction enhancements — To simplify setting the start and end times of a redaction segment, the Start and End boxes support minutes and seconds.  
• Reports — Added the Sharing Audit Report that lists all user actions related to sharing evidence and cases, for a configurable date range. |
| May 2016 Rev. A                   | • In the Groups Administration section, information about the external ID of a group is available in the following procedures:  
  o Search and View Groups  
  o Edit Group Members, Monitors, and Other Settings  
• Minor changes to the View Case page are reflected in the View Case procedure, in addition to the Share a Case with Other Users in Your Agency, Share a Case by Download Link, and Share a Case with a Partner Agency procedures. |
**Release Name and Document Revision**

<table>
<thead>
<tr>
<th>Release Name and Document Revision</th>
<th>Revision description</th>
</tr>
</thead>
</table>
| April 2016                        | • Accelerated video playback — Updated the Playing Video and Audio Evidence section with information about playing videos faster or slower.  
• Redaction enhancements — Updated the Video Evidence Redaction section to reflect changes to the video redaction tool suite.  
• View Evidence page enhancements — Updated the Working with Any Evidence section to reflect minor changes to the View Evidence page.  
• Reassignment of cases to groups — Updated the Reassign Cases section to provide information about reassigning a case to a group. |
| March 2016 Rev. A                 | • Adding information about the simplified case acceptance changes, which enables an agency to receive shared cases from partner agencies without having to manually accept each shared case. For more information, see Receiving Shared Cases from Partner Agencies.  
• Added information about the Axon Capture mobile app. Axon Capture replaces the Evidence Mobile app. |
| February 2016 Rev. A             | • The Supported Web Browsers section includes updated information about support for Internet Explorer and about disabling the Compatibility View setting.  
• The Working with Image Evidence section includes new information about using the photo edit feature.  
• The Viewing Document Evidence section includes new information about viewing PDF document evidence in Evidence.com.  
• The Device Search — All Devices and My Devices section includes new information about how to search for unassigned devices. |

**Release 1.31 and Earlier Document Versions**

The following table provides information about versions of this guide that describe Evidence.com release 1.31 and earlier.

<table>
<thead>
<tr>
<th>Document version</th>
<th>Revision date</th>
<th>Revision description</th>
</tr>
</thead>
</table>
| 23               | 1/26/2016     | Release 1.31:  
• The Supported Web Browsers section includes updated information about end of support for Internet Explorer 8.  
• The Video Evidence Redaction section includes updated information about the following, new features available in manual redactions only:  
  o Audio redaction  
  o Blur level selection including blackout, configurable per redaction mask  
• The Axon Device Manager for Axon Body 2 Cameras section includes updated information about the general availability of the Axon Device Manager app in the Google Play store. |
<table>
<thead>
<tr>
<th>Document version</th>
<th>Revision date</th>
<th>Revision description</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>12/8/2015</td>
<td>Release 1.30:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added information about end of support for Internet Explorer 8.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updated the User Administration section with information about the following topics:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Simplified user states to Active and Inactive.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Ability to pre-provision Inactive users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Ability for administrators to control user account information and prohibit users from updating their own information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Add User and Import Users feature updates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Changes to deactivating users: reassigning evidence and devices when a user status is changed to Inactive is now optional rather than mandatory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updated the Media Player Controls section with information about the video quality selector feature.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updated the Video Evidence Redaction section with information about the following topics:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Simplified redaction workflow, including a more visible Extract button.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Keyboard shortcuts for precise placement of redaction mask-segment handles.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Added information about image tools that are available to agencies who request early access.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added information about the new Axon device assignment app that is available to agencies who request early access.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updated information about user audit trails, which are now available in CSV format in addition to PDF. See User Audit Trail.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Renamed the TASER Video Settings page to the Camera Settings page, with new settings for Axon Body 2. See Configure Body Camera Settings.</td>
</tr>
<tr>
<td>21</td>
<td>10/27/2015</td>
<td>- Updated information regarding adding and removing tags from evidence and cases.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updated the Partner Agency Administration section, to reflect the changes the Partner Agencies page.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added information about the audio and video file types supported by the Evidence.com media player. For more information, see Playing Video and Audio Evidence.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Revised and expanded the Case Management section.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Added the Partner Contact Search permission to Appendix A: Roles and Permissions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updated the Working with Markers and Clips section to reflect the name change of the Media Player tab to “Clips &amp; Marker”.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Updated the Video Evidence Redaction section to reflect the name change of the Redactor tab to “Redactions”.</td>
</tr>
<tr>
<td>20.1</td>
<td>9/23/2015</td>
<td>Corrected the name of the assisted redaction feature.</td>
</tr>
<tr>
<td>Document version</td>
<td>Revision date</td>
<td>Revision description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>----------------------</td>
</tr>
</tbody>
</table>
| 20.0             | 9/22/2015    | **1.28 Release:**  
|                  |              | • Added detailed information about using the new redaction tools, including manual redaction and assisted redaction. For more information, see Video Evidence Redaction.  
|                  |              | • Added the Supported Web Browsers section.  
|                  |              | • Added the Change Language section, which describes how users can select the language that Evidence.com uses when they sign in to your agency.  
|                  |              | • Revised the name of the “Fields & Retention” link on the Admin page to “Fields & Retention Categories”. Affected sections include Evidence ID Validation and Categories and Evidence Retention Policies.  
|                  |              | • Revised information about permissions required to share evidence and cases, in Appendix A: Roles and Permissions. Specifically, sharing by download link and sharing with authenticated users in other agencies require separate permissions. |
| 19.0             | 8/25/2015    | **1.27 Release:**  
|                  |              | • Added information about the new media player.  
|                  |              | • Moved information about the traditional media player and its tools, including redaction, to an appendix.  
|                  |              | • Added information about evidence ID validation.  
|                  |              | • Updated CSV file format information for Import Groups, because files now require header rows.  
|                  |              | • Updated information about the Help section. |
| 18.0             | 7/28/2015    | **1.26 Release:**  
|                  |              | • Updated look and feel, to reflect the site refresh of all Evidence.com agencies.  
|                  |              | • Added the Import Groups, Members, and Monitors section.  
|                  |              | **Other revisions:**  
|                  |              | • Revised and expanded the Roles and Permissions section, including the new Appendix: Roles and Permissions.  
|                  |              | • Revised and expanded the Categories and Evidence Retention Policies section.  
|                  |              | • Revised and expanded the Evidence Management section. |
| 17.0             | 6/23/15      | **1.25 Release:**  
|                  |              | • Added the Groups Administration section  
|                  |              | • Updated information about search page names and behavior  
<p>|                  |              | • Updated the User Administration section |</p>
<table>
<thead>
<tr>
<th>Document version</th>
<th>Revision date</th>
<th>Revision description</th>
</tr>
</thead>
<tbody>
<tr>
<td>16.0</td>
<td>5/26/15</td>
<td>1.22 Release:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sharing with partner agencies is limited to one agency at a time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Password Reset is available on user search results page</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bulk video redaction, additional options</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.23 Release:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Partner agency setup changes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reporting interface changes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1.24 Release:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Menu bar and other navigational changes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dashboard changes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User Summary report support for single user reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Evidence Search &quot;View All&quot; button removed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bulk Evidence Sharing by unauthenticated download link</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Case Creation support for adding evidence with the same ID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Case Invite page added for management of case invitations from partner agencies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reporting support for Internet Explorer</td>
</tr>
<tr>
<td>15.0</td>
<td>2/20/15</td>
<td>1.21 Release: Case Sharing Enhancements, Bulk Over-Redaction, Clip &amp; Redaction enhancements: backend processing, Tagged with AXONClip or AXONRedact, More detailed audit logs; Bulk download can exceed 4.2GB for zip files, Reports Enhancements</td>
</tr>
<tr>
<td>14.0</td>
<td>1/12/2015</td>
<td>1.20 Release: Active directory beta, clips and redacted files will now be created as new, separate pieces of evidence.</td>
</tr>
<tr>
<td>13.0</td>
<td>11/11/2014</td>
<td>1.19 Release: Updated Interagency Case Sharing, user reporting, bulk download to ISO file, extend retention duration without changing category, agency admin audit log</td>
</tr>
<tr>
<td>12.0</td>
<td>10/7/2014</td>
<td>Updated content based on 1.17 and 1.18 release: External case sharing, bulk download, IP whitelisting, expire all passwords, Reporting service, and change username.</td>
</tr>
<tr>
<td>11.0</td>
<td>11/4/2013</td>
<td>Updated content based on the Evidence.com 1.16 release</td>
</tr>
<tr>
<td>10.0</td>
<td>1/23/2013</td>
<td>Updated Settings Options, Categories &amp; Retention, Devices Menu Options and screenshots based on the Evidence.com 1.15 release.</td>
</tr>
<tr>
<td>9.0</td>
<td>8/2/2012</td>
<td>Updated Settings Options, Import Evidence, Help Center topics and all relevant screenshots, and added a topic on Search based on the Evidence.com 1.14 release.</td>
</tr>
<tr>
<td>8.0</td>
<td>5/1/2012</td>
<td>Updated content and screenshots based on the Evidence.com 1.13 release</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Created a separate AXON Pro ETM Setup Guide and removed that content from this document.</td>
</tr>
<tr>
<td>7.0</td>
<td>3/8/2012</td>
<td>Updated content and screenshots based on the Evidence.com 1.12 release.</td>
</tr>
<tr>
<td>6.0</td>
<td>11/7/2011</td>
<td>Updated content and screenshots based on the Evidence.com 1.11 release.</td>
</tr>
<tr>
<td>5.0</td>
<td>8/17/2011</td>
<td>Updated content and screenshots based on the Evidence.com 1.10 release</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Merged content from the Quick Start Guide.</td>
</tr>
<tr>
<td>Document version</td>
<td>Revision date</td>
<td>Revision description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>4.0</td>
<td>4/15/2011</td>
<td>Functionality test steps added.</td>
</tr>
<tr>
<td>3.0</td>
<td>4/12/2011</td>
<td>Installing ETM instructions added.</td>
</tr>
<tr>
<td>2.0</td>
<td>3/16/2011</td>
<td>Updated document for flow, format and content.</td>
</tr>
<tr>
<td>1.0</td>
<td>3/14/2011</td>
<td>Initial Document.</td>
</tr>
</tbody>
</table>