



Axon Evidence User and Administrator Reference Guide

Evidence.com June 2022 Release
Evidence.com Version 2022.6
Document Revision: A

Apple and Safari are trademarks of Apple, Inc. registered in the US and other countries.

iOS is a trademark or registered trademark of Cisco.

Firefox is a trademark of The Mozilla Foundation registered in the US and other countries.

Google, Google Play, Android, and Chrome are trademarks of Google, Inc.

Microsoft, Windows, Edge, and Excel are trademarks of Microsoft Corporation registered in the US and other countries.

JavaScript is a trademark of Oracle America, Inc. registered in the US and other countries.


 Axon, Axon Body, Axon Capture, Axon Citizen, Axon Commander, Axon Device Manager, Axon Evidence, Axon Fleet, Axon Flex, Axon Interview, Axon Investigate, Axon Performance, Axon Respond, Axon Signal, Axon View, TASER, TASER 7, X2, and X26P are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information, visit www.axon.com/legal. All rights reserved. ©2022 Axon Enterprise, Inc.

Table of Contents

What's New	18
Introduction	19
About This Guide.....	19
Administrator Overview	20
Implementation Checklist.....	20
Supported Web Browsers	21
Sign In to Axon Evidence	21
Dashboard	22
Critical Device Alerts	23
Evidence Management	23
Upcoming Evidence Deletions.....	23
Case Management	24
System Usage	24
Managing Your User Account	24
Update Your Basic Account Information	25
Verify Your Mobile Phone Number.....	26
Change Your Password	27
Change Language.....	28
Update Your Email Notifications.....	28
Viewing My Groups Information	29
Axon Citizen	30
Axon Citizen for Communities Workflow:.....	31
Axon Citizen for Officers Workflow:	31
Axon Citizen Permissions and Settings Information	32
Example Axon Citizen Management Permissions	33
Citizen Evidence and Portal Details Page Overview	34
Creating a Public Portal	38
Editing a Public Portal.....	40
Closing a Public Portal	41
Instructions for Evidence Collectors	41
Using Axon Capture to Invite an Individual	41

Using Axon Evidence to Invite an Individual	43
Virus Scan for Axon Citizen	45
Submission Notifications	46
Using Axon Evidence to Triage Submissions	46
Searching for Axon Citizen Evidence in Axon Evidence	49
Additional Information on Citizen Evidence Detail Pages	49
What Community Members See	51
Public Portal	51
Individual Invite – Phone	52
Individual Invite - Email	55
Evidence Management	57
Import Evidence	57
Supported File Types	60
Evidence Search — All Evidence, My Evidence, and Shared Evidence	61
Evidence Search Filters	62
Review Mode	65
Evidence Access Control Overview	67
User Access to Evidence and User Permissions	68
Evidence Search Page Views	70
Access List Information	71
Providing Access to Evidence Outside Your Organization	72
Access Classes and Categories	72
Changing Evidence Access Class	73
Changing Evidence Access Class from the Evidence Search Page	73
Changing Evidence Access Class from the Evidence Detail Page	76
Removing a Restricted or Confidential Access Class from Evidence	79
Changing Evidence Access	80
Adding Users and Groups to an Inside My Agency Access List from the Evidence Search Page	80
Adding Users and Groups to an Outside My Agency Access List from the Evidence Search Page	82
Providing Evidence Outside My Agency by Unauthenticated Download Link from the Evidence Search Page	85

Adding Users and Groups to the Inside My Agency Access List from the Evidence Detail Page	87
Modifying an Inside My Agency Access List.....	91
Removing Users and Groups from the Evidence Access List.....	93
Adding Users, Groups, and Agencies to the Outside My Agency Access List	94
Modifying and Removing Users and Groups on the Outside My Agency Access Lists.....	98
Working with Evidence Search Results.....	101
View Evidence	101
Request Access.....	102
Bulk Update ID	102
Bulk Add Categories to Evidence	103
Bulk Add Tags to Evidence.....	103
Reassign Evidence.....	104
Bulk Video Redaction.....	105
Bulk Download Evidence.....	106
Download Speed Information	108
Delete Evidence.....	108
Restore Evidence.....	109
Export Evidence Search Results	109
Working with Any Evidence.....	110
Third-Party Video Support	110
Metadata Overlays.....	112
Edit Title and ID	116
Add or Edit Evidence Categories	116
Edit Recorded Date and Time.....	117
Download Evidence File	118
Flag or Un-Flag Evidence	118
Add to or Remove Evidence from a Case	118
Reassign Evidence.....	119
View Evidence Audit Trail.....	119
Delete Evidence.....	120
Restore Deleted Evidence	120
Extend a Retention Date	121

Assign and Un-Assign Categories	121
Add and Remove Tags for Evidence	122
Edit Location	123
Edit Description	123
Notes and Evidence	124
View Evidence with Same ID	125
Viewing Video Source Information	125
Viewing Document Evidence	126
PDF Viewer Controls	126
PDF Viewer Actions	127
Playing Video and Audio Evidence	127
Internet Connection Speed Recommendations	127
Media Player Controls	128
Media Player Actions	130
Multicam Playback	131
Selecting Videos for Playback	131
Viewing Multiple Videos	133
Combined Multicam Video Extraction	134
Requesting Human Transcriptions	134
Transcript Status	135
Sharing Transcripts	136
Working with Markers and Clips	136
Marker and Clip Controls	138
Hypermedia Markers	139
Add a Marker	140
View a Marker	140
Edit a Marker	141
Download a Marker	141
Export a Marker Report	142
Add a Clip	142
Play a Clip	143
Edit a Clip	144
Extract a New File from a Clip	144

Delete a Marker or Clip	145
Video Evidence Redaction (Legacy Redaction Tools).....	146
Manual Redaction	147
Smart Tracker Assisted Redaction	150
Redaction Workflow Comparison	153
Create a Redaction Manually	154
Edit a Redaction	156
Create a Redaction with Smart Tracker Assisted Redaction	158
Extract a Redacted Video from a Redaction	160
Delete a Redaction.....	161
Skin Blur Redaction.....	162
View Evidence Extracted from Clips, Markers, and Redactions	163
Working with Image Evidence	164
Photo Edit Controls.....	164
Photo Edit Workflow	165
Create a Photo Edit.....	165
Edit a Photo Edit.....	166
Extract an Edited Image	168
Evidence Map.....	169
Basic Map Actions	169
Searching from the Evidence Map.....	170
Publish to Social Media	171
Publish to Social Media Permission.....	171
Publishing to Social Media.....	172
Axon Auto-Transcribe.....	174
Auto-Transcribe Workflows	175
Auto-Transcribe Accuracy	175
Auto-Transcribe Licensing.....	176
Auto-Transcribe Permissions	176
Fast Evidence Review.....	178
Requesting an Auto-Transcript	178
Using Fast Evidence Review.....	181
Miranda Warning Detector	183

Auto-Transcribe Bulk Requests	183
Bulk Requests from the Evidence Search Page	183
Bulk Requests from the Case Details Evidence Tab	184
Transcription Assistant.....	186
Transcription Assistant Editing Actions.....	187
Transcript Verification	193
Keyboard Controls	195
Transcription Assistant Settings.....	195
Foot Pedal Support	197
Sharing Transcriptions	198
Auto-Transcribe Audit Events	199
Redaction Studio and Redaction Assistant.....	201
Redaction Studio Terms and Concepts	201
Redaction Studio Layout and Controls.....	203
Keyboard Controls	204
Redaction Studio Best Practices.....	204
Using Redaction Studio for Video and Audio Redaction.....	205
Using Redaction Studio for Audio Extracts	211
Using Redaction Studio for PDF Document Redaction	212
Document Redaction Best Practices	212
Redacting a PDF Document.....	213
Using Redaction Studio Annotation Tools	216
Adding an Outline Marker	217
Adding a Text Box	218
Using Redaction Studio for Image Redaction.....	220
Redaction Activity Report	221
Using Redaction Assistant.....	223
Redaction Assistant Settings	223
Starting Redaction Assistant.....	224
Reviewing Redaction Assistant Masks.....	226
Case Management	228
Creating a Case.....	228
Searching Cases.....	230

Working with Case Search Results.....	231
Export Case Search Results	231
Case Search Results Bulk Actions	232
View a Case	234
Case Details Page	235
Export a Case Audit Log	235
Add Evidence to a Case	236
Import Evidence to a Case	239
Summary Tab.....	241
Edit the Case ID, Description, Owner, or Retention of a Case	241
Add and Remove Tags for a Case	242
Case Notes	243
Evidence Tab.....	243
Pin Evidence.....	243
Case Evidence Filters	244
Remove Evidence from a Case.....	246
Working with Evidence Folders	246
Working with Evidence in a Case	251
Evidence Bulk Actions.....	252
View a Case Map	254
Case Access Control Overview	255
User Access to Case and User Permissions.....	255
Case Search Page Views.....	256
Access List Information	257
Evidence Access vs Case Access.....	259
Changing Case Access Class	259
Changing case Access Class from the case Detail Page.....	259
Removing a Restricted or Confidential Access Class from a Case	262
Granting Case Access	263
Adding Users and Groups to an Inside My Agency Access List from the Case Search Page	263
Modifying an Inside My Agency Case Access List	266
Removing Users and Groups from the case Access List.....	268

Sharing Cases Outside Your Agency.....	269
Shared Case Retention Information.....	270
Share Case to Users or Groups Within a Partner Agency	270
Updating a Shared Case.....	275
Send a Download Link.....	277
Inventory and Device Management	280
Device Search — All Devices and CEWs	281
Device Search Filters.....	282
Working with Device Search Results.....	283
Update Device Status	283
Update Device Home.....	285
View Device Profile.....	285
View Device Assignee	285
Export Device Search Results.....	286
Working with a Device	286
Assign a Device.....	288
View Evidence Created by a Device	289
Edit Device Settings	289
Device Audit Trail Information	290
TASER 7 Health	292
TASER 7 Usage Dashboards.....	293
Vehicle Search.....	294
Add a New Fleet 3 Vehicle.....	294
Add a New Fleet 1 or 2 Vehicle.....	296
Add Multiple New Vehicles	298
Edit Vehicle Information.....	300
Bulk Assign Devices.....	301
Axon Device Manager.....	303
Returns.....	304
Returns Permissions.....	304
Accessing the Returns Page	305
Returns Page Overview	306
Reviewing Submitted and Completed Returns	307

Creating a New Return	308
Canceling a Return	314
Reporting	316
Run a Report	318
Downloading Reports	319
Download Report from Reports Page	320
Download Report from Email Download Link.....	320
Example Data Aggregation Using Microsoft Excel Pivot Tables.....	320
System Status Page	321
Administrator Overview.....	323
User Administration	323
User Account Statuses.....	324
User Account Added as Active.....	325
User Account Added as Inactive	325
Active User Account During Password Reset	325
Add Users.....	325
Add One User	326
Add Many Users	327
Complete the User Registration Process	330
Re-Invite Users.....	331
Deactivate Users	332
Deactivate Many Users.....	332
Deactivate One User.....	333
Reactivate Users.....	334
Reactivate Many Users	334
Reactivate One User	335
Unlock a User Account	336
Reset Passwords and Security Questions.....	336
Reset Password and Security Questions from a User Details Page.....	336
Reset Passwords and Security Questions for Users from User Search Results	337
Change a Username	337
Edit Other User Account Information.....	338
User Audit Trail.....	339

Get a User Audit Trail	340
Expire All Passwords.....	341
Groups Administration.....	341
Groups and Membership	342
Managing Group Access.....	343
Monitoring Evidence with Groups	343
Group States	345
Permissions and Groups.....	345
Implementing Groups	346
Update Roles and Permissions	347
User Permissions	347
Group Management and Audit Permissions.....	348
Create a Group	348
Import Groups, Members, and Monitors.....	351
Strategies for Importing Groups, Members, and Monitors	351
Import Groups.....	352
Define Members and Monitors.....	354
Search and View Groups	357
Dashboard List for Monitors	358
My Profile Page for Members and Monitors	358
User Accounts of Members and Monitors.....	358
Edit Group Members, Monitors, and Other Settings	359
View All Evidence.....	360
View Group Audit Trail.....	360
Delete Group	361
Delete Group from Group Search Results.....	361
Delete Group from Group Profile Page	361
Evidence Groups	362
Using Evidence Groups	362
Example Evidence Group Setup and Scenarios.....	363
Permissions and Evidence Groups.....	365
Assigning Users to Evidence Groups.....	366
Manually Assigning Evidence to an Evidence Group.....	368

Command Hierarchy	369
Command Hierarchy Permissions	369
Command Hierarchy Management Permission	370
Command Hierarchy Evidence Management Permissions	370
Creating a Command Hierarchy	370
Manually Creating a Command Hierarchy	371
Importing a Command Hierarchy	372
Exporting and Editing a CSV file	373
Creating a CSV file	374
Importing a CSV File	375
Editing a Command Hierarchy	376
Manually Editing a Command Hierarchy	376
Importing Updates for a Command Hierarchy	378
Agency Profile	380
Configure Agency Address	380
Configure Agency Logo	381
View Agency Audit Trail	382
Partner Agency Administration	384
Invite an Agency to Share with Your Agency	385
Accepting or Rejecting an Invitation to Collaborate with an Agency	386
Ending Collaboration with a Partner Agency	387
Removing an Agency from your Can Share to My Agency List	387
Removing an Agency from your My Agency Can Share To List	387
Categories and Evidence Retention Policies	388
Special and Pre-Configured Categories	388
Evidence Retention Policy	389
Restricted and Confidential Categories	389
Add a Category	390
Edit a Category	391
Delete a Category	393
Field Validation	393
Configure Field Validation	394
Disable Evidence ID Validation	396

Regular Expressions for Field Validation.....	396
Example Regular Expressions	397
User Experience	398
Evidence Playback Settings.....	398
Roles and Permissions	400
Planning Roles	402
Add a Role	402
Edit a Role.....	403
Copy a Role	404
Assign a Role to Users	404
Ranks.....	405
Add a Rank	405
Edit a Rank.....	406
Delete a Rank.....	407
Reorder Ranks	408
Citizen Settings.....	409
Configure Citizen Settings.....	410
Device Home	412
Add a Device Home.....	413
Edit a Device Home.....	414
Delete a Device Home	415
Custom Metadata	416
Viewing Information about Custom Metadata.....	416
Create a Custom Metadata Field.....	418
Editing a Custom Metadata Field	419
Human Transcription Service	420
Human Transcription Service Setup.....	421
Redaction Settings	424
Create a Redaction Disclaimer	424
Enable and Disable Redaction Disclaimers	425
Delete Redaction Disclaimers.....	425
Case Settings	425
Devices and Applications Settings	427

Configure Body Camera Settings	428
Early Access Devices	429
Add a Device to the Early Access List	429
Remove a Device from the Early Access List	430
Body Camera Wi-Fi Networks	430
Adding a Body Camera Wi-Fi Network	430
Editing a Body Camera Wi-Fi Network	431
Deleting a Body Camera Wi-Fi Network	431
Configure Fleet Settings	431
Configure CEW Settings	432
TASER 7 Settings	433
TASER 7 CQ Settings	434
TASER X2 & X26P Settings	435
Signal Configuration	437
Configure Signal Vehicle Settings	437
Configure Fleet Hub Signal Settings	438
Configure CEW Signal Settings	440
Configure Signal Sidearm Settings	441
Signal Sidearm Registration	442
Register and Assign on Evidence.com	442
Axon Respond Settings	443
Evidence Upload XT Settings	443
Axon View Settings	445
Axon Capture Settings	446
Security Settings	448
IP Security	449
IP Allowed Lists for Multi-Homed Networks	450
Axon Application Exceptions	451
Multi-Factor Authentication	452
Critical Action Permissions	453
Multi-Factor Authentication Account Settings	454
Configure Password Settings	454
API Settings	455

Active Directory—Single Sign On	457
Help Section.....	458
Help Center	458
Release Notes and User Guides.....	458
Download and Install Evidence Sync.....	458
Download Axon Capture	460
Download Evidence Upload XT	460
Contact Us	461
Appendix A: Roles and Permissions	462
Permission Reference.....	462
Pre-Configured Roles and Default Permissions.....	475
Pre-Configured Lite Roles and Default Permissions	479
Appendix B: Traditional Media Player	483
Appendix C: Body Camera and Fleet Camera Settings.....	484
Body Camera Settings	484
Axon Body 3 Camera Settings Descriptions.....	484
Axon Body 2 and Axon Flex 2 Camera Settings	490
Axon Body and Axon Flex Camera Settings	493
Fleet 3 Settings	494
Video Settings.....	494
Audio Settings.....	495
Lights Settings	496
Location Settings.....	496
Respond Livestreaming Settings.....	496
Activation Settings	497
Device Management.....	497
Evidence Review.....	497
Upload Settings	498
User Permissions	498
Fleet 1 & 2 Settings	499
Video Settings.....	499
Audio Settings.....	500
Activation Settings	501

Offload Settings.....	501
-----------------------	-----

What's New

This guide includes the following changes, made in support of the June 2022 updates to Axon Evidence:

- Updated the [Playing Video and Audio Evidence](#) section to include information about the brightness and contrast controls.
- Updated the [Working with Markers and Clips](#) section to show how to export a Marker Report and to update the maximum number of characters for marker descriptions.
- Renamed Auto-Transcribe Review Assistant to Fast Evidence Review in the [Axon Auto-Transcribe](#) section.
- Updated [Appendix A: Roles and Permissions](#) to include the new Edit Agency Device Settings permission.
- Added [Audio in Video Recall setting](#) information to the Axon Body 3 Camera Settings Descriptions section.

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

- [Evidence.com June 2022 Release Notes](#)

Note: The guide revision history was removed from the document to save space. If you have questions about the guide revision history, contact Technical Support to request the information.

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 Body-Worn Cameras integrate easily with Evidence.com.

Transport

The transport element consists of Axon Dock, Axon Evidence Upload XT, and Evidence Sync. Axon Dock functions as the docking, charging, and upload station for Axon body worn cameras. Evidence Upload XT is a Windows®-based desktop application that enables users to easily upload non-Axon generated digital evidence to their agency's Axon Evidence.com account. Evidence Sync is a Windows-based desktop application provides a secure interface for uploading and managing TASER Conducted Energy Weapon (CEW) generated logs as well as TASER CAM and Axon videos.

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 Axon 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

Axon Evidence supports the latest stable release (except where noted) of the following browsers:

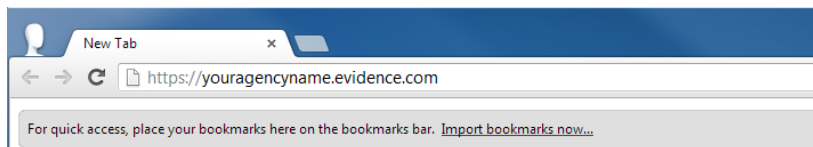
- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Safari

Sign In to Axon Evidence

To sign in to Axon Evidence, 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`

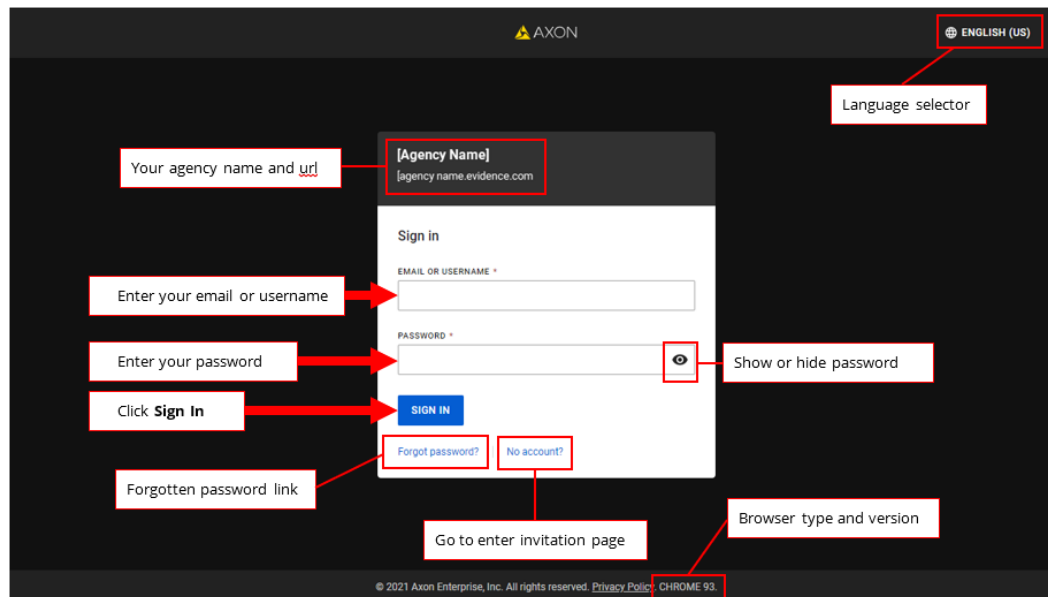


Your agency's sign in page appears.

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

After signing in for the first time, Axon recommends you add a browser bookmark to your agency site.

Note: If you sign in to Axon Evidence 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 assigned Role and permissions, you may not see all of these sections.

- Critical Device Alerts
- Evidence management, with links to My evidence and Evidence shared with me
- Upcoming Evidence Deletions, with links to My evidence deletions and All evidence deletions
- Case management, with links to My cases and Cases shared with me
- My account, with links to [My profile](#) and [My groups](#)
- Axon Citizen (see [Axon Citizen](#) for more information)
- Axon Performance (see [Axon Performance](#) in the Axon Help Center for more information)
- System Usage – linked at the top of the page

Critical Device Alerts

The Critical Device Alerts section only appears if there are any devices with critical errors.

Click the **View critical devices** link to be taken to the Inventory page with the list of devices with critical errors.

It is recommended that you do not use devices listed under Critical Device Alerts and that you return the devices or contact Technical Support for additional information.

Evidence Management

The Evidence management section has two links:

- My evidence – takes you to the My Evidence search page
- Evidence shared with me – takes you to the Evidence search page and shows all evidence shared with you

Upcoming Evidence Deletions

The Upcoming Evidence Deletions section has two links:

- My evidence deletions – takes you a list of evidence owned by you that has been scheduled for deletion.

- All evidence deletions – take you to a list of all evidence that is scheduled for deletion.

Evidence can be scheduled for [deletion manually](#) or in accordance with the retention duration of the category that is assigned the evidence. For more information on automatic deletion, see [Categories and Evidence Retention Policies](#).

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

If you want to prevent evidence from being deleted, you can [restore the evidence](#).

Case Management

The Case management section has two links:

- My cases – takes you to the My Cases search page
- Cases shared with me – takes you to the Shared Cases page

System Usage

Clicking the System Usage link at the top of the dashboard takes you to the System usage page.

This page provides information about your agency's account usage, including:

- License limits – this shows the number of Pro and Basic licenses for your agency (how many are used and how many are remaining) and storage limits.
- The System Usage summary includes evidence added in the last 30 days, broken out by video, audio and other types expressed in gigabytes (GB)
- 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 also displays the total number of Evidence.com users and your agency's active devices.
- The Active Devices summary the type and number of active devices at your agency.

Managing Your User Account

In most agency configurations, users can manage and update many settings for their own user accounts.

The default permissions assigned to the User role allows a user to edit their account information. However, some agencies do not allow users to perform any of the procedures in this section, such as changing username and email address. Check with your Axon Evidence.com administrator learn what permissions are enabled for your account.

Update Your Basic Account Information

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

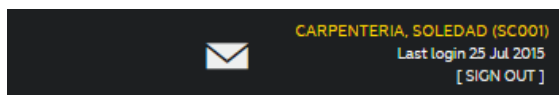
- Badge ID
- First Name
- Last Name
- Username
- Language
- Time Zone
- Email address
- Phone number

If enabled by your agency, you can also view information about your assigned Rank and Evidence Group. However, you cannot edit this information.

Your account profile page may also include tabs for updating your email notifications and viewing your group-related lists.

To access your profile page:

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



The My profile page with your User Information is shown.

2. Below the User Information section, click **Edit**.
3. Update your information as needed.

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

4. Click **Save**. You are asked to enter your password to verify the changes.

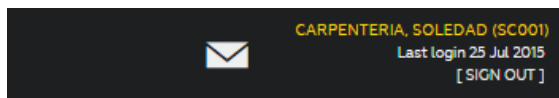
Above User Information, a banner message about the success of the updates appears.

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.



The My profile page with your User Information is shown.

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

2. If you have not entered a phone number or need to change the number, follow the action below. Otherwise, skip to step 3.
 - Click **Edit**.
 - Update your phone number information as needed.
 - Click **Save**. You are asked to enter your password to verify the changes.

3. Click **Verify phone number**.

A dialog box displays the verification method options, which are a SMS Text message or a voice Call.

4. Select the verification method you want to use to receive the 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.

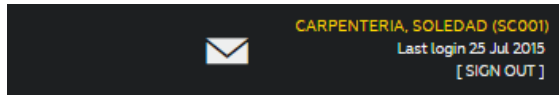
5. Use your mobile phone to receive the verification code.
6. In the **Code** box, type the verification code and then click **OK**.
7. On the notification message box, click **OK**.

Your mobile phone is verified.

Change Your Password

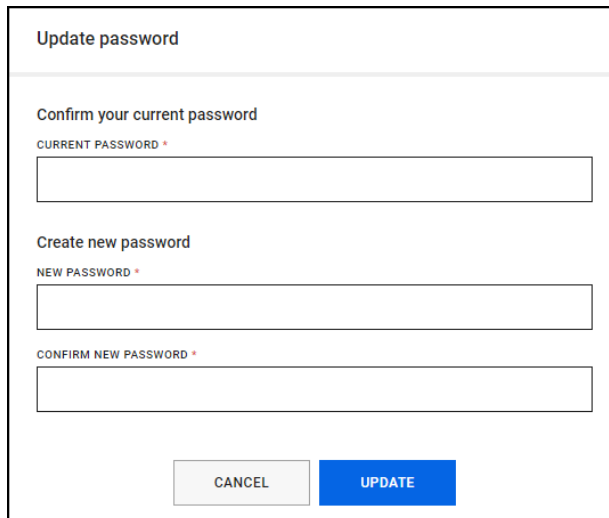
Generally, you can change your password as needed. However, your agency may have added certain password configuration requirements for your password. Contact your agency's Axon Evidence.com administrator for information about password requirements.

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



The My profile page with your User Information is shown.

2. Under Security Settings, click **Update Password**. The Update Password dialog box is shown.

A white dialog box titled 'Update password' with a light grey border. Inside, the text 'Confirm your current password' is followed by a red asterisk and the label 'CURRENT PASSWORD *'. Below this is a white text input field. The next section is 'Create new password', followed by a red asterisk and the label 'NEW PASSWORD *', with another white text input field below it. A third section is 'CONFIRM NEW PASSWORD *' with a third white text input field. At the bottom, there are two buttons: a grey 'CANCEL' button and a blue 'UPDATE' button.

3. Type your password in the **Current Password** field.
4. Then type your new password in the **New Password** field and type it again in the **Confirm New Password** field.
5. Click **Update**.

A banner message notifies you about the success of the password change.

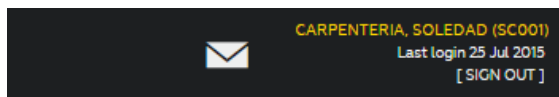
Note: If your agency uses the Minimum Password Age setting, you will not be able to change your password again until that time is reached. If needed, you can still request that an agency administrator reset your password so that you can change it.

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 My Profile 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 My profile page with your User Information is shown.

2. Below the User Information section, click **Edit**.
3. In the **Language** list, click the language that you want to use.
4. Click **Save**. You are asked to enter your password to verify the changes.
5. Sign out and then sign in to your Evidence.com agency again.

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

Update Your Email Notifications

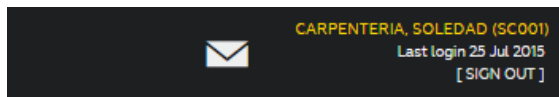
You can set personal preferences for email notifications. The email notifications that are available to you are determined by the role assigned to your user account. You may not see all of the email notification settings.

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.



The My profile page with your User Information is shown.

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.

Viewing My Groups Information

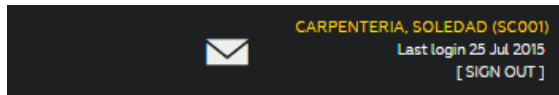
If you are a group monitor or a member of a group, the My Group section user's profile page will show the following group-related lists.

- **Groups I monitor** — Appears if you have monitoring permission for a group.
- **Groups I am a member of** — Appears if you are a member of any group.

You can access the group profile page by clicking the group title.

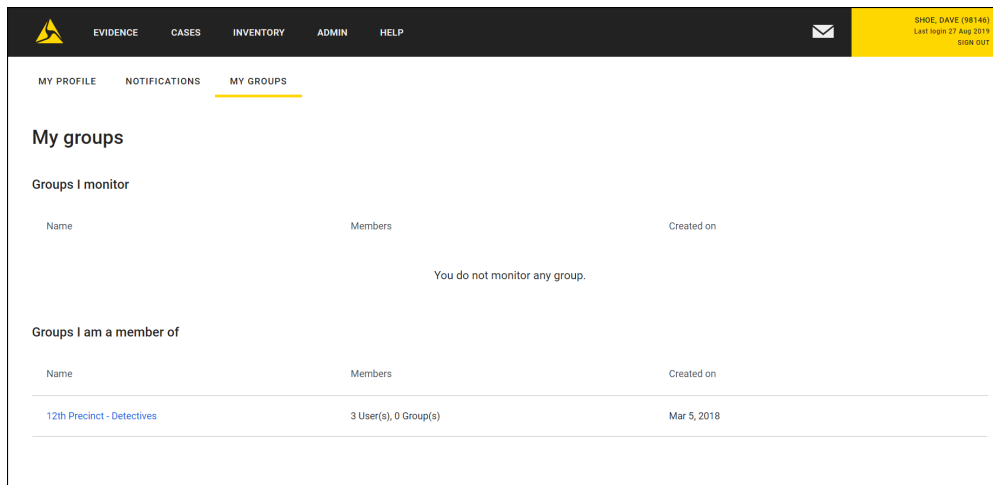
To access your profile page:

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



The My profile page with your User Information is shown.

2. On the second menu bar, click **My Groups**.



The list of groups you monitor and are a member of is shown. Click the group title to go to the group profile page.

Axon Citizen

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

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 Axon Evidence 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 Axon Evidence.
2. The community member uploads files and Axon Evidence 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 Axon Evidence. 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 Axon Evidence 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.

Citizen Management			
View Portals (Individual & Public)	<input checked="" type="radio"/> ANY PORTAL	<input type="radio"/> ONLY THEIR OWN	<input type="radio"/> PROHIBITED
Invite Individual Pro	<input checked="" type="radio"/> ALLOWED	<input type="radio"/> PROHIBITED	
Create Public Portal	<input checked="" type="radio"/> ALLOWED	<input type="radio"/> PROHIBITED	
Edit and Close Public Portal	<input checked="" type="radio"/> ANY PORTAL	<input type="radio"/> ONLY THEIR OWN	<input type="radio"/> PROHIBITED
Triage Submissions	<input checked="" type="radio"/> ANY PORTAL	<input type="radio"/> ONLY THEIR OWN	<input type="radio"/> PROHIBITED
Audit Trail PDF	<input checked="" type="radio"/> ANY PORTAL	<input type="radio"/> ONLY THEIR OWN	<input type="radio"/> PROHIBITED

- **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 Axon Evidence 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.

Use case	View portal	Invite individual	Create public portal	Edit and close public portal	Triage submissions
Patrol officers that can invite individuals and must triage their own submissions	Only Their Own	Allowed	Prohibited	Prohibited	Only Their Own
Detectives that can create public portals and triage their own submissions.	Only Their Own	Allowed	Allowed	Only Their Own	Only Their Own

Use case	View portal	Invite individual	Create public portal	Edit and close public portal	Triage submissions
Someone in the public information office that can create a public portal, but <i>not</i> triage themselves.	Any Portal	Prohibited	Allowed	Any Portal	Prohibited
You have a centralized group that can triage any portal.	Any Portal	Prohibited	Prohibited	Prohibited	Any Portal
Command staff that can access and triage any portal.	Any Portal	Allowed	Allowed	Any Portal	Any Portal

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 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.

Citizen Evidence					
CREATE PUBLIC PORTAL + INVITE INDIVIDUAL					
Public Portals Show Filters					
ID	CREATED	TITLE	OWNER	PORTAL INFO	STATUS
reporter-test	04/21/2022 10:48	Reporter Integration Test Portal		View Summary (0 Items)	No Submissions
77594-3	04/14/2022 14:05	Something wild happened.		View Summary (0 Items)	No Submissions
test1241254125	04/12/2022 17:01	test		View Summary (0 Items)	No Submissions
test1234124	04/12/2022 16:59	test		View Summary (0 Items)	No Submissions
SS-publicportal	10/19/2021 10:37	Scranton Strangler strikes again!		View Summary (1 Item)	Accepted
1127-081221	08/12/2021 13:27	this is the title of this fake incident		View Summary (0 Items)	No Submissions
hehe	08/04/2021 02:36	hehe dha		View Summary (1 Item)	Declined
asfasdf	09/15/2020 02:32	asf		View Summary (1 Item)	Declined
test-cctv	09/15/2020 02:21	testing cctv		View Summary (0 Items)	No Submissions
testdha	09/15/2020 02:14	testdha		View Summary (0 Items)	No Submissions
<div> < 1 2 > </div> 14 Results					
Individual Invites Show Filters					
ID	CREATED	CITIZEN INFO	OWNER	PORTAL INFO	STATUS
thumbo #1	04/27/2022 13:37	gray, davy (dcarrell@axon.com)		View Summary (1 Item)	Accepted
None	04/25/2022 09:14	a (+12069407952)		View Summary (0 Items)	No Submissions
None	04/22/2022 16:50	a (spropemnick@axon.com)		View Summary (0 Items)	No Submissions
test	04/22/2022 09:34	Unidentified		View Summary (0 Items)	No Submissions
Reporter test po...	04/21/2022 11:13	Joe (mjamesson@axon.com)		View Summary (1 Item)	Accepted
hahahahahaehu...	04/13/2022 14:35	Awesomeness, Graham Awesome (g...		View Summary (0 Items)	No Submissions
None	04/12/2022 21:08	gstinson@gmail.com		View Summary (0 Items)	No Submissions
None	04/12/2022 21:07	Unidentified		View Summary (0 Items)	No Submissions
None	04/12/2022 21:05	Barrel, Ole Biscuit (gstinson@gmail.c...		View Summary (0 Items)	No Submissions
None	04/12/2022 21:04	Ftangftang (+12062280740)		View Summary (0 Items)	No Submissions
<div> < 1 2 3 4 5 6 ... 8 > </div> 71 Results					

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 Axon Evidence after a submission is uploaded.

- In Axon Evidence 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:

thumbo #1

Submission from davy gravy

Sent via [redacted] [AUDIT TRAIL](#)

EVIDENCE SUMMARY		INFO
0 untriaged item(s)	1 accepted item(s)	<p>CREATED ON: Apr 27, 2022 1:37 PM</p> <p>CREATED BY: [redacted]</p> <p>CITIZEN INFO: [redacted]</p> <p>CATEGORIES: 2 thousand y...</p> <p>DESCRIPTION: Hamburglar snatchin' yo patties up</p>

EVIDENCE LIST		
FILE TYPE	CAPTION	STATUS
JPEG image	No Caption	Auto-Accepted

- 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:

The screenshot displays the 'Portal Details' page for a public portal. The page is divided into several sections:

- Header:** Includes the title 'Something wild happened.' and links for 'AUDIT TRAIL' and 'VISIT PUBLIC PORTAL'.
- EVIDENCE SUMMARY:** Shows '0 untriaged Item(s)', '0 accepted Item(s)', and '0 total Item(s)'.
- SHARE PUBLIC LINK:** Includes a toggle switch for 'Open for submissions' and a 'COPY' button with a public link: <https://sb-pro.ag1.evidence.com/axon/citizen/pu...>
- PORTAL SETTINGS:** A table listing various settings for the portal.

SETTING	VALUE
TITLE	Something wild happened.
ID	77594-3
CATEGORIES	A thousand y...
DATE	
DESCRIPTION	This is a description for the portal. Let's look at where this all goes.
LOCATION	21114 80th Ave W, Edmonds, WA, 98026, USA
OWNED BY	[User Avatar]
CREATED ON	Apr 14, 2022 2:05 PM
CREATED BY	[User Avatar]
ALLOW EMAIL	Disabled
- Map:** A map showing the location of the portal at 21114 80th Ave W, Edmonds, WA, 98026, USA. The map includes a street view and a location pin.

- 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 Axon Evidence account.
2. On the dashboard page, under Axon Citizen, 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.

The screenshot shows the 'Create Public Portal' page within the Axon Evidence application. The top navigation bar includes 'EVIDENCE', 'CASES', 'INVENTORY', 'REPORTS', 'ADMIN', and 'HELP'. A user profile for 'SCHUER, DAVID (DS101)' is visible in the top right corner. Below the navigation bar, a sub-menu shows 'ALL EVIDENCE', 'MY EVIDENCE', 'SHARED EVIDENCE', 'EVIDENCE MAP', 'IMPORT EVIDENCE', and 'CITIZEN EVIDENCE'. The main content area is titled 'Create Public Portal' and contains several form fields: 'PUBLIC URL' (with a placeholder 'incident-url' and a generated URL below it), 'ID', 'LOCATION OF INCIDENT' (with a map icon and 'No Location Added'), 'CATEGORIES' (a dropdown menu), 'PORTAL OWNER' (with a placeholder 'Enter last name, first name, badge ID, or email address'), 'TITLE' (with a placeholder 'Enter a short title summarizing the incident'), 'DESCRIPTION' (a large text area with a placeholder 'Enter a description of the incident for the public'), and 'DATE AND TIME' (with a placeholder 'Select date/time'). A 'SUBMIT' button is located at the bottom left of the form.

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.

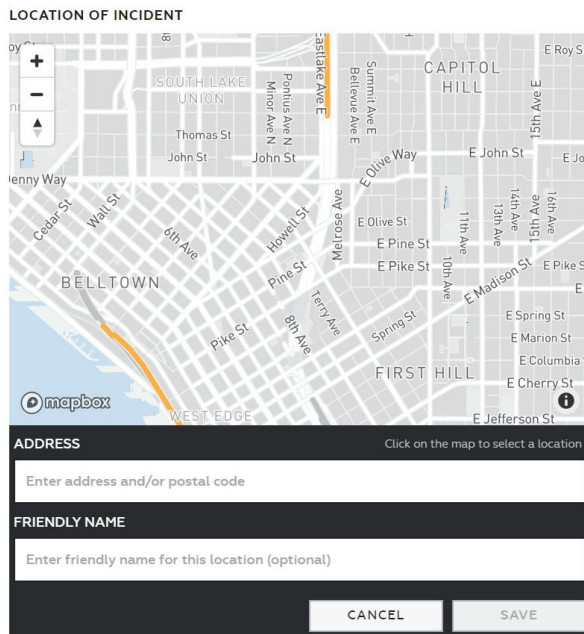
4. Enter the **ID** as required by your agency.
5. Add evidence **Categories** as needed. A public portal can have multiple categories.

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, Axon Evidence 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 Axon Evidence 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.

LOCATION OF INCIDENT



Click on the map to select a location

Enter address and/or postal code

FRIENDLY NAME

Enter friendly name for this location (optional)

CANCEL SAVE

- 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 Axon Evidence 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.

Edit Public Portal

PUBLIC URL *

<https://sb-pro.qa.evidence.com/axon/citizen/public/2ndandjacksonhitandrum>

ID *

CATEGORIES *
 X

PORTAL OWNER *
 X

TITLE *

DESCRIPTION *

DATE AND TIME

SAVE

LOCATION OF INCIDENT

 320 2nd Avenue South
 Seattle, Washington 98104, United States

4. Change the portal information as needed.

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

5. Click **Save**.

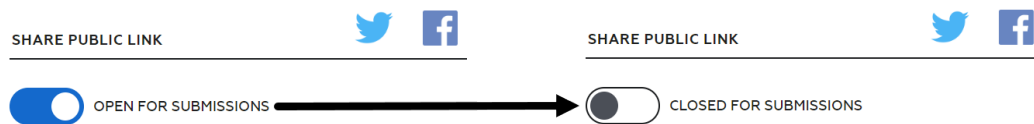
You are taken to the Portal Details Page. From here you can copy and share the portal link on social media and other websites. The Portal Details Page is also used to close the portal when it is no longer needed.

Closing a Public Portal

1. Sign in to your Axon Evidence 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 Axon Evidence. Axon Evidence 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.

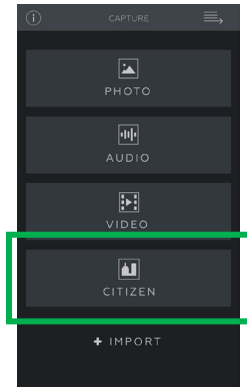
Note: For agencies that have French set as their default language in Axon Evidence, the Axon Citizen individual invite text, Terms of Use, and Privacy Policy information will also appear in French.

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 Axon Evidence.

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.

Note: For categories with set retention periods, the retention countdown begins when the evidence file is uploaded, not when the file was created.

5. Enter the **Description** as needed. The Description field is used by the person sending the invitation to provide additional information about the incident to the recipient. The Description field has a maximum length of 2,000 characters.

Note: Descriptions that exceeds 603 characters, including spaces, will be trimmed in the text message or email. The full description will be visible to the community member when they visit the Axon Citizen submission portal page.

6. 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.

7. If allowed by your agency, you can select to store a contact's information in Axon Evidence.

If email was selected as the delivery method, the contact's information is always stored in Axon Evidence.

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

8. If the contact's information should be stored, enter the name and birth date information for the contact.
9. 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.

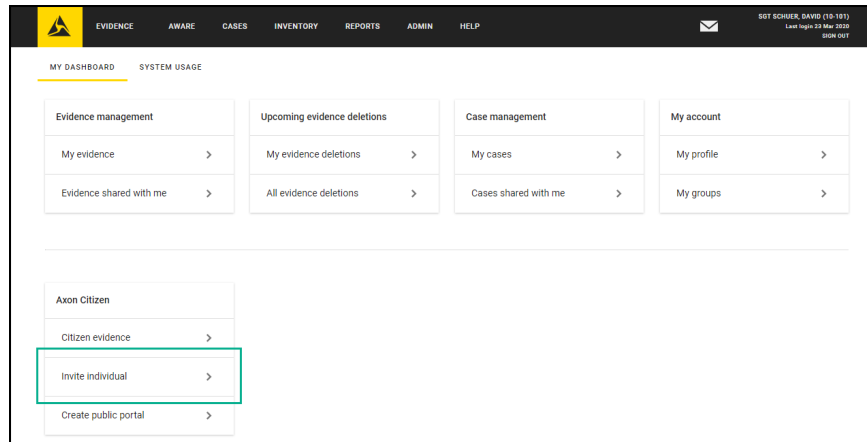
After the contact uploads the submission, you will receive an email message from Axon Evidence. If your agency requires you to triage submissions, you can use the link in the email to go to the triage page for the submission.

10. 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 Axon Evidence to Invite an Individual

1. Sign in to your Axon Evidence account.

- On the dashboard page, under Axon Citizen, click **Invite Individual**.



Alternately, on the menu bar, click **Evidence**, then click **Citizen Evidence**, and then click **Invite Individual**.

- On the Individual Invite page, enter the **ID** or NA as required by your agency.

 A screenshot of the 'New Individual Invite' form. The top navigation bar is the same as the dashboard. Below the navigation bar, there are tabs for 'ALL EVIDENCE', 'MY EVIDENCE', 'SHARED EVIDENCE', 'EVIDENCE MAP', 'IMPORT EVIDENCE', and 'CITIZEN EVIDENCE'. The 'CITIZEN EVIDENCE' tab is selected. The form title is 'New Individual Invite'. It contains several sections: 'Incident' with an 'ID' field (placeholder '##-###'), a 'CATEGORIES' dropdown menu, and a 'DESCRIPTION' text area with the placeholder 'Enter a description of the incident for the recipient.' Below this is 'Community Member Information' with a 'DELIVERY METHOD' dropdown menu (placeholder 'Select a delivery method') and a 'SUBMIT' button.

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

Note: For categories with set retention periods, the retention countdown begins when the evidence file is uploaded, not when the file was created.

5. Enter the **Description** as needed. The Description field is used by the person sending the invitation to provide additional information about the incident to the recipient. The Description field has a maximum length of 2,000 characters.

Note: Descriptions that exceeds 603 characters, including spaces, will be trimmed in the text message or email. The full description will be visible to the community member when they visit the Axon Citizen submission portal page.

6. 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.
7. If allowed by your agency, select if the contact's information should be stored in Axon Evidence.

If email was selected as the delivery method, the contact's information is always stored in Axon Evidence.

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

8. 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 Axon Evidence. 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. 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 Axon Evidence. Files that pass the scan can be managed normally in Axon Evidence, 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.

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, Axon Evidence sends an email notification to the owner. However, for public portals, if Axon Evidence receives additional submissions for a portal before the user visits and triages the portal, then additional emails are not sent to that user.

Using Axon Evidence to Triage Submissions

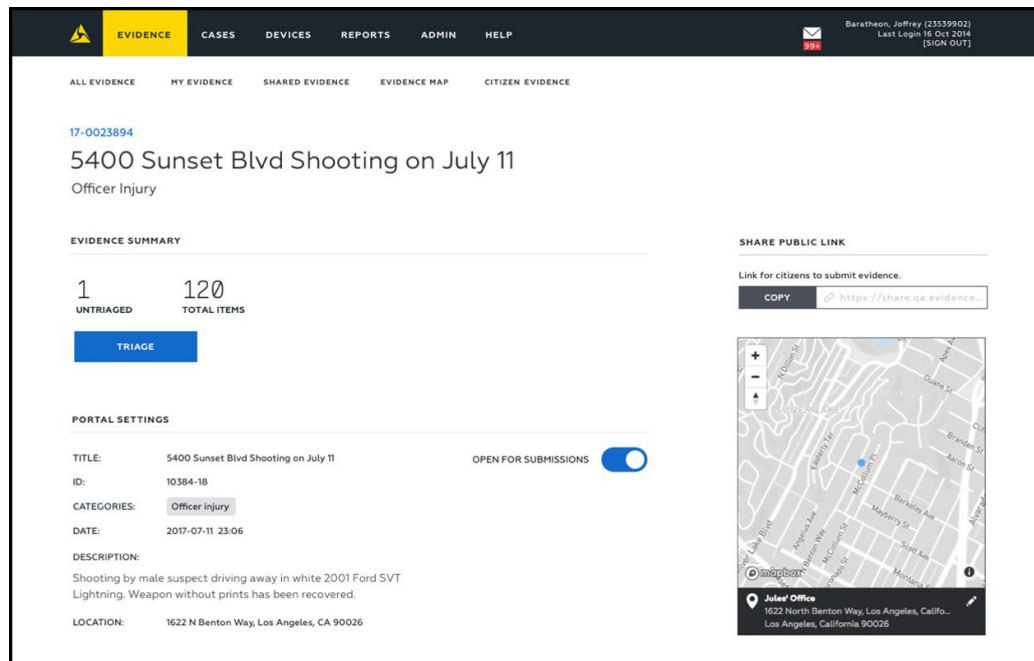
Use the following procedure to review and accept or decline community submissions.

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 Axon Evidence after a submission is uploaded. The email lists the ID, categories, and number of untriaged items in the submission.

- In Axon Evidence, 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.

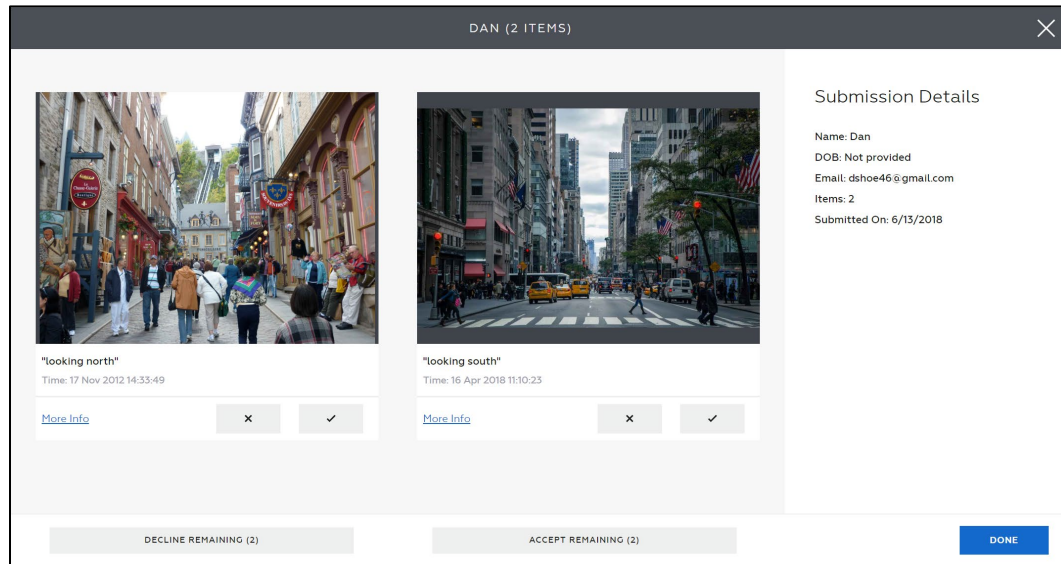
Note: The example image below shows a Public Portal Detail Page. Individual invite pages show different information, but the instructions to review submissions are the same.



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.



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 Axon Evidence

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.

TAG

AXONCitizen

X

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.

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 Axon Evidence, 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 Axon Evidence, 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).

CITIZEN METADATA		CITIZEN METADATA	
Status:	Accepted	Status:	Accepted
Name:	Jones, Don	Name:	Not provided
DOB:	Jul 4, 1982	DOB:	Not provided
Phone:	+12069151016	Phone:	Not provided
Caption:	"Just before accident"	Caption:	Not provided

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.

5	27 Feb 2018	08:21:04 (-08:00)	Community Member: John T Doe Phone Number: +12065364541	Evidence successfully created via Axon Citizen. Link Secret: mnKz0A5Kcuv4MNN3nPhMugZANQWv5i48hUDi7zSTCUD C Portal ID: 8ab5d9c8f0f54b3ab449240cf2470b2d Incident ID: 18-2018 Caption: N/A File Name: 15197484436775490348212307948475.jpg
4	20 Feb 2018	02:08:08 (-08:00)	Community Member: Unidentified (name not provided)	Evidence successfully created via Axon Citizen. Link Secret: 7SL3A1q01fONF9c9aYi65yuKJvVL2WtWKgxraT9vQa91 Portal ID: 9afc59c6de384a02bae536f51340820d Incident ID: N/A Caption: Altoona shehsbsbsh File Name: image.jpg

What Community Members See

Public Portal

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

Notes:

- For agencies that have French set as their default language in Axon Evidence, the Axon Citizen upload screen text, Terms of Use, and Privacy Policy information will also appear in French.
- If your agency has enabled Help Contact Settings, the information is shown in the footer of the evidence submission screen.

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.

The left screenshot displays a 'Thank you for helping the SB-PRO-QA' message. Below the message is a 'SUMMARY OF INCIDENT' box containing the following details:

SUMMARY OF INCIDENT	
INCIDENT July 11 Incident at 2nd Ave and Jackson	
DATE 7/11/18	TIME 10:30 pm
DESCRIPTION We are looking for information about a hit and run that occurred at the corner of 2nd Ave and S. Jackson Street. Please submit photos or videos of the incident.	

At the bottom of the page are links for 'Privacy Policy' and 'Terms of Use', and a blue 'SUBMIT EVIDENCE' button.

The right screenshot displays a 'Thank you for assisting us.' message. Below the message is a form to provide contact information:

MOBILE PHONE NUMBER (REQUIRED) *

United States (+1) Phone Number

☒ Provide my information
Sharing your contact information allows our investigators and prosecutors to more effectively use your evidence.

FIRST NAME (OPTIONAL)
First

MIDDLE NAME (OPTIONAL)
Middle

LAST NAME (OPTIONAL)
Last

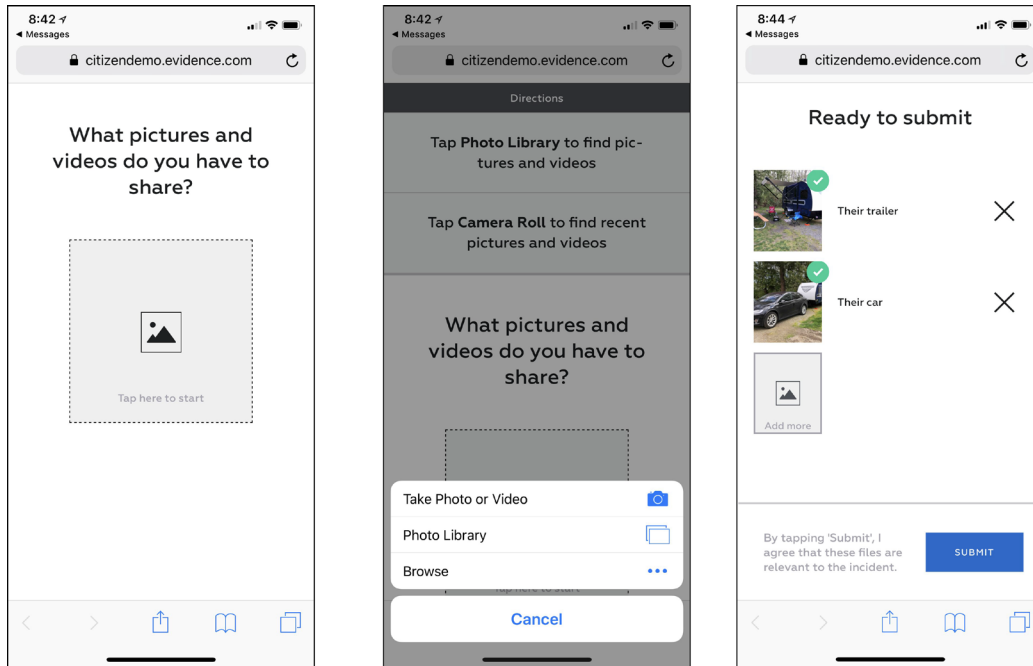
BIRTHDATE (OPTIONAL)
MM DD YYYY

At the bottom of the page are links for 'Privacy Policy' and 'Terms of Use', and a blue 'SEND LINK' button.

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.



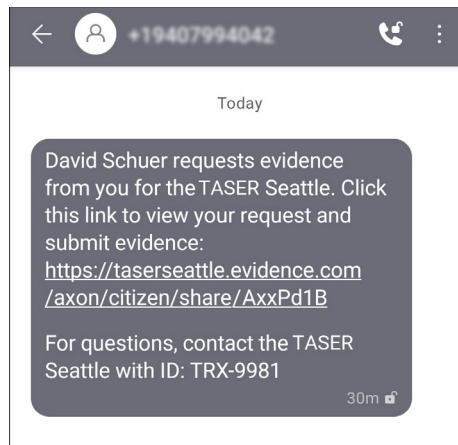
After the community member has added all their files and the files are uploaded to the website, they tap **Submit** to transfer the files to your agency's Axon Evidence account and then can close their browser.

Individual Invite - Phone

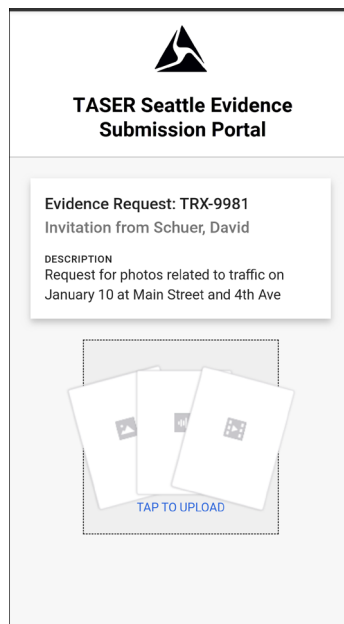
This section provides an overview of what a community member sees and how they interact with an individual invite sent to their phone.

Note: If your agency has enabled Help Contact Settings, the information is shown in the footer of the evidence submission screen.

- 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.

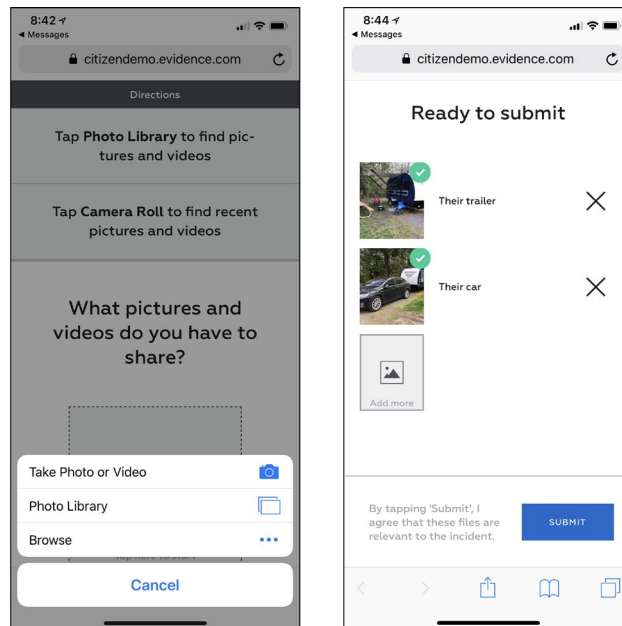


- The first screen welcomes them and by tapping **Tap to Upload**, they can upload their files.

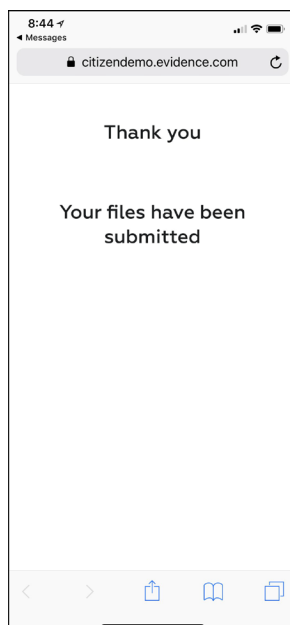


- The community member can add files for uploading. They also have the option of adding a caption for each file. More files can be added by tapping **Add Files**. Each

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 Axon Evidence account and then can close their browser.

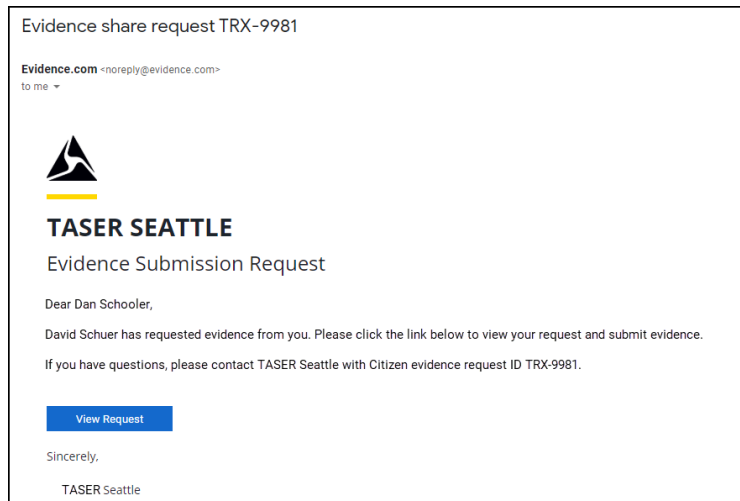


Individual Invite - Email

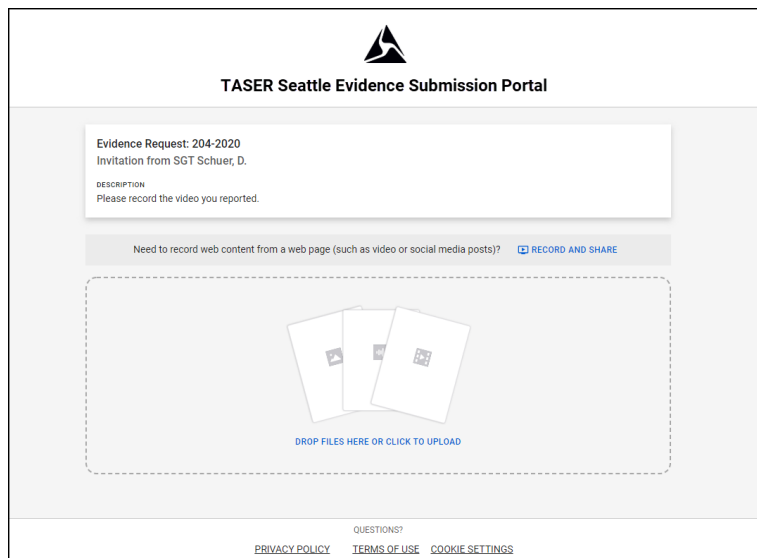
This section provides an overview of what a community member sees and how they interact with an individual invite sent to their email.

Note: If your agency has enabled Help Contact Settings, the information is shown in the footer of the evidence submission screen.

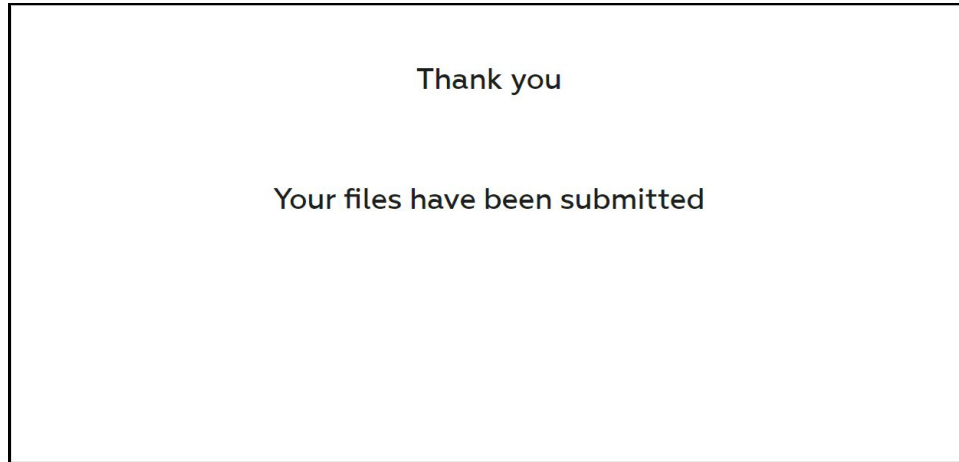
- After the invite is sent, the citizen receives the email message with the private link. Clicking **View Request** takes them to a website where they can upload files.



- From the upload page, the community member can add files for uploading. They can also record and share webpage information. They also have the option of adding a caption for each file. 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 click **Submit** to transfer the files to your agency's Axon Evidence account and then can close their browser.



Evidence Management

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

Import Evidence

Users who are allowed the Upload External Files permission can import evidence files into your Evidence.com agency. This can be done by uploading files or by recording website content like a social media post or YouTube video. 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 (video, image, audio or document) based on the file extension. 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 4 Gigabytes.

1. On the menu bar, click **Evidence**. Below the search filters, click **Import Evidence**.

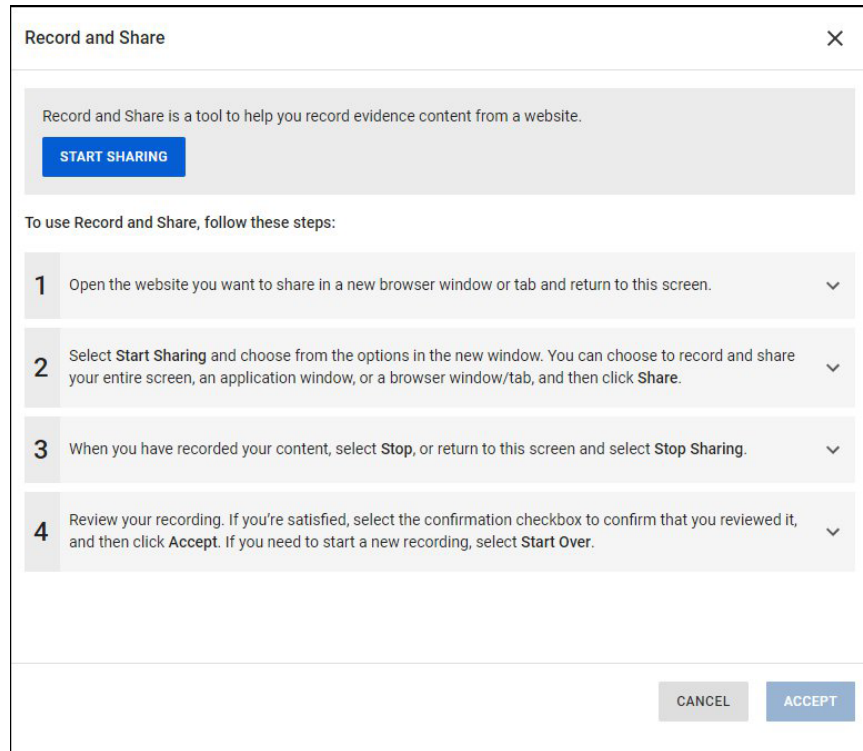
The Import Evidence page appears.

The screenshot displays the Axon Evidence web application interface. At the top, a dark navigation bar contains the Axon logo and menu items: EVIDENCE, RESPOND, CASES, INVENTORY, REPORTS, ADMIN, and HELP. A 'SIGN OUT' link is visible on the right. Below this, a secondary navigation bar shows tabs for ALL EVIDENCE, MY EVIDENCE, SHARED EVIDENCE, EVIDENCE MAP, and CITIZEN EVIDENCE. The main content area features a search filter section with fields for ID, TITLE, USER OR GROUP, DATE (with Start and End date pickers), CATEGORY (a dropdown menu), and TAG (a dropdown menu). There is also a CUSTOM METADATA text input field and a 'SHOW ADVANCED SEARCH' link. To the right of the filters are 'RESET FILTERS' and a blue 'SEARCH' button. At the bottom of the page, a summary bar shows 'Evidence' with '31,709 results'. On the right side of this bar, the 'IMPORT EVIDENCE' button is highlighted with a green rectangular box, followed by an 'EXPORT RESULTS' button and a three-dot menu icon.

2. To add files that you want to import, use either of the following methods:
 - Find the files on your computer and then drag and drop the files onto the Import Evidence page.
 - Click **Choose Files** and then use the dialog box to find and select the files on your computer.

You can add up to 500 files at one time.

3. To record website content, click **Record and Share**,
 - A panel on the right side of the page. In the same browser type open a new browser window or tab and go to the website you want to record.



- Click **Start Sharing**, select the window or tab to record, and if audio should be recorded.
- When you are ready to stop recording, click **Stop** in the selected tab/window or **Stop Sharing** in the panel.
- Review the recording and, if needed, start over. You can add a Title, Evidence ID, and Category, as needed. Once you are ready to accept the recording, select the checkbox and click **Accept**.

Repeat this step to record other website content.

4. Once the files are added, you can edit the Title, ID and Category information individually for each file. You can also edit the IDs and Categories for all the imported evidence or

select and edit the IDs and Categories for specific files using the **Edit All IDs** and **Edit All Categories** options.

If your agency has evidence ID field validation enabled, it is enforced when files are uploaded.

Information	Purpose
Title	A meaningful name for the evidence. If you omit the title, Evidence.com assigns the file name as the title.
ID	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 add it to the case.
Category	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.

Import Evidence

Drag and Drop
[CHOOSE FILES](#)

4 Files EDIT ALL IDS EDIT ALL CATEGORIES UPLOAD

<input type="checkbox"/>	TITLE	ID	CATEGORY	FILE SIZE	PROGRESS	
<input type="checkbox"/>	Original view.jpg	####-####		1.9 MB	Hasn't started yet	
<input type="checkbox"/>	Action photo.jpg	####-####		50.1 KB	Hasn't started yet	
<input type="checkbox"/>	Missing Person photo.bmp	####-####		1.0 MB	Hasn't started yet	
<input type="checkbox"/>	External view.jpg	####-####		0.4 MB	Hasn't started yet	

Online streaming and preview features supported in Evidence.com for the following file types:
 video: DIVX, TS, 3GP, ASF, AVI, FLV, MOV, MP4, RM, VOB, WMV, F4V, MPEG, MPG
 image: JPEG, JPG, GIF, PNG, BMP, TIF, TIFF, ARW, CR2, CRW, SRF, NEF, NRW, ORF, HEIC, DNG, RAF
 audio: MP3, WAV
 document: PDF

Other digital media types can be uploaded and maintained in Evidence.com but online preview features are not currently supported.
 File Size must be less than 4.0 GB

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.

5. Click **Upload**.

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

If an upload fails, you can use the Retry option to try to upload the files without having to choose the files again.

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

Supported File Types

This section lists the document, image, video, and audio file types supported for viewing in Evidence.com. It is possible other file types can be viewed in Evidence.com, but only the file types listed in this section are specifically supported. Note that if [Third-Party Video Support](#) is enabled for your agency, other video formats are available.

Document Files

Axon Evidence supports viewing PDF document files.

Image Files

The following image file types are supported in Axon Evidence:

ARW, BMP, CR2, CR3, CRW, DNG, GIF, HEIC, JPEG, JPG, NEF, NRW, ORF, PNG, RAF, SR2, SRF, TIF, and TIFF.

Video Files

The following video file types are supported by the Axon Evidence media player:

.3gp, .3gpp, .3g2, .asf, .avi, .divx, .f4v, .flv, .mov, .mpeg, .mpg, .mp4, .m4v, .qt, .ram, .rm, .ts, .tts, .vob, .webm, .wma, .wmv

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 Files

The following audio file types are supported by the Axon Evidence:

.mp2, .mp3, .m4a, .mpga, .wav

For actions available for all file types, regardless of media player support, see [Working with Any Evidence](#).

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.

The screenshot displays the Evidence Search interface. At the top, there is a navigation bar with tabs: EVIDENCE, RESPOND, CASES, INVENTORY, REPORTS, ADMIN, and HELP. Below this, a sub-navigation bar shows: ALL EVIDENCE, MY EVIDENCE, SHARED EVIDENCE, EVIDENCE MAP, and CITIZEN EVIDENCE. The main search area includes several input fields: ID, TITLE, USER OR GROUP, DATE (with Start and End date pickers), CATEGORY (dropdown), and TAG (dropdown). There is also a CUSTOM METADATA field. Below these are several filter sections with checkboxes: FILE TYPE (Video, Audio, Document, Image, Firing Log, Zip, Other), STATUS (Active, Processing, Queued for Deletion, Excluded, Deleted, Declined, Pending Triage), USER ASSOCIATION (Uploaded By, Owner, Access List), DATE TYPE (Recorded On, Uploaded On, Deleted On), SOURCE (Body Worn Cameras, Fleet, CEWs, Other), and ACCESS CLASS (Unrestricted, Restricted, Confidential). There are also checkboxes for FLAG (Flagged, Not Flagged) and DEVICE SERIAL, VEHICLE, and MOUNT ORIENTATION. At the bottom left, it says 'Evidence 0 results'. At the bottom right, there are links for 'IMPORT EVIDENCE', 'EXPORT RESULTS', and a 'SEARCH' button.

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.

Task	Steps
View evidence	In search results, click the title of the evidence that you want to view.
Find evidence that you own	Click My Evidence .
Find evidence that is shared with you	Click Shared Evidence .

Task	Steps
Change search results	<ol style="list-style-type: none"> 1. Update the evidence search filters. For more information, see Evidence Search Filters. 2. Click Search.
Sort search results	<p>Use the Sort By list to select ID, Title, Uploaded Date, or Recorded Date and click Sort Order to change order.</p> <p>When in Table view, click the column headings for ID, Title, Uploaded Date, or Recorded Date.</p>
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.
- **Custom Metadata** – Limits search results to evidence with custom metadata that includes the characters you entered. This field is only available if Custom Metadata is enabled for your agency.

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.

Note: Excluded status was previously used by the Evidence Sync application to exclude evidence from showing up in search results. This status is no longer used by Sync or other Axon applications and is only relevant to evidence uploaded by Sync when it was used.

- **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.
- **Access Class** – Limits search results to evidence access class selected. By default the search results include all access class types.
- **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 Axon Fleet 3, 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.
- **Evidence Group** – Limits search results to the selected Evidence Group.

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.

102
ITEMS FOUND

VIEW TYPE

GALLERY

TABLE











SORT BY

UPLOADED ON

SORT ORDER

Az ↑

Za ↓

<input type="checkbox"/>	ID	TITLE	RECORDED BY	OWNER	UPLOADED ON ↑	RECORDED ON	CATEGORY	STATUS	
<input type="checkbox"/>	2016100915355	 [Clip 1.1] AXON Body 2 ...	 Maddie Eiden (2301)	Maddie Eiden (2301)	03 Nov 2015 22:14:92	03 Nov 2015 22:14:92	2m 1s	DUI	Active
<input type="checkbox"/>	2016100915355	 AXON Body 2 Video 20...	 Maddie Eiden (2301)	Maddie Eiden (2301)	03 Nov 2015 22:14:92	03 Nov 2015 22:14:92	37m	Officer Training	Active
<input type="checkbox"/>	2016100910213	 Screen Shot 2016-07-0...	 Anshuman Srivastava (31...	Anshuman Srivast...	03 Nov 2015 22:14:92	03 Nov 2015 22:14:92		DUI, Officer Training...	Active
<input type="checkbox"/>	2016100910323	 AXON Body 2 Video 20...	 Josh Hepfer (4834)	Josh Hepfer (4834)	03 Nov 2015 22:14:92	03 Nov 2015 22:14:92	1h 32m	Officer Training	Active
<input type="checkbox"/>	2016100904134	 (Extraction 1.2) Screen ...	 Dan Bellia (9804)	Dan Bellia (9804)	03 Nov 2015 22:14:92	03 Nov 2015 22:14:92		DUI	Active

102 ITEMS FOUND

VIEW TYPE: ☒ GALLERY ☐ TABLE

SORT BY: SORT ORDER:

☐ SELECT 20 ITEMS ON PAGE

Video-10-20-4354356.mp4 38s

Michelle Guarino (2901)

ID 49290192-891289

RECORDED ON 05/20/2016 12:21:20

CATEGORY DUI, Training officer, a...

Video-10-20-4354356.mp4 38s

Michelle Guarino (2901)

ID 49290192-891289

RECORDED ON 05/20/2016 12:21:20

CATEGORY DUI, Training officer, a...

Video-10-20-4354356.mp4 38s

Michelle Guarino (2901)

ID 49290192-891289

RECORDED ON 05/20/2016 12:21:20

CATEGORY DUI, Training officer, a...

Video-10-20-4354356.mp4 38s

Michelle Guarino (2901)

ID 49290192-891289

RECORDED ON 05/20/2016 12:21:20

CATEGORY DUI, Training officer, a...

Video-10-20-4354356.mp4 38s

Michelle Guarino (2901)

ID 49290192-891289

RECORDED ON 05/20/2016 12:21:20

CATEGORY DUI, Training officer, a...

Review Mode

Review Mode make it easier to review related pieces of evidence at one time. Review Mode is a carousel-type experience for quickly viewing and flipping through sets of digital evidence. This allows users to select and view multiple evidence files at one time, without having to open the Evidence Detail page for each piece of evidence.

Review Mode can be launched from the All Evidence, My Evidence, Shared Evidence, or Evidence Map search pages.

1. [Search for the evidence files](#) you want to review.
2. Select the video, image, PDF document, and audio evidence on the search page and then click **Review**.

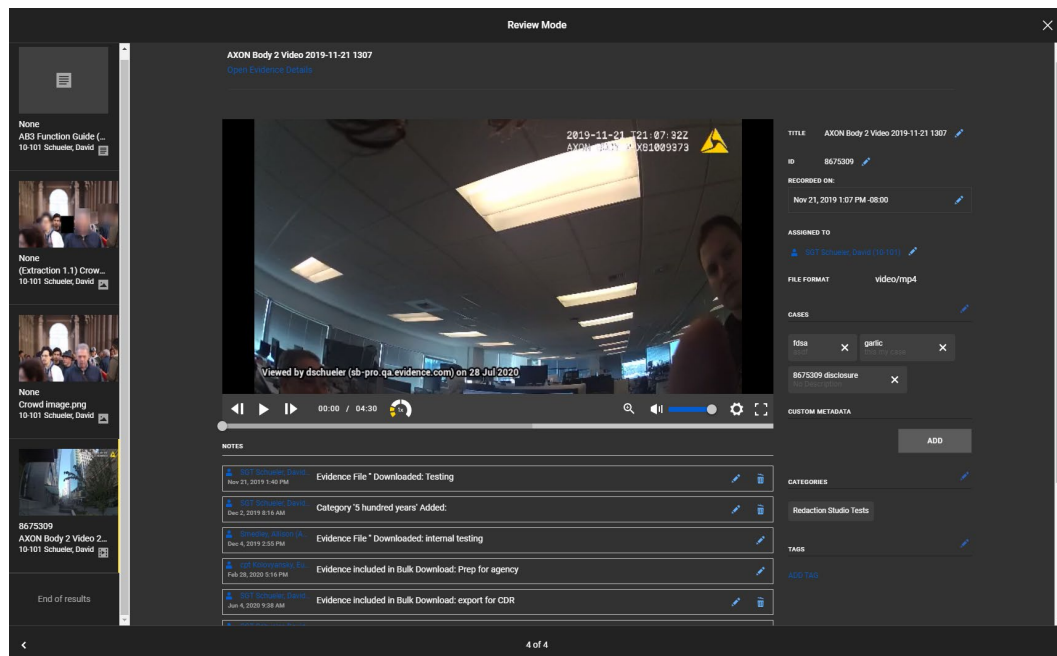
The screenshot shows the Axon Evidence web application. At the top is a navigation bar with tabs: EVIDENCE, RESPOND, CASES, INVENTORY, REPORTS, ADMIN, and HELP. Below this is a sub-navigation bar with: ALL EVIDENCE, MY EVIDENCE, SHARED EVIDENCE, EVIDENCE MAP, and CITIZEN EVIDENCE. The main area contains a search form with fields for ID, TITLE, USER OR GROUP, DATE (Start/End), CATEGORY, and TAG. There is also a CUSTOM METADATA field and a SHOW ADVANCED SEARCH link. A RESET FILTERS button and a blue SEARCH button are at the bottom right of the search section. Below the search section, the 'Evidence' section shows 533 results with 4 selected. A 'REVIEW' button is highlighted with a green box. To the right of the REVIEW button are links for UPDATE ID and ADD CATEGORY. Below this is a table of evidence items.

ID	TITLE	OWNER	UPLOADED BY	UPLOADED ON	RECORDED ON	CATEGORY	STATUS
None	VIDEO 2020-07-29 10-101	SGT Schueler, David (10-...	SGT Schueler, ...	Jul 29, 2020 2:45 PM	Jul 29, 2020 10:43 AM	23s	1 day delete Active
12-072901	PHOTO 2020-07-29 10-101	SGT Schueler, David (10-...	SGT Schueler, ...	Jul 29, 2020 2:43 PM	Jul 29, 2020 10:41 AM	AI Training, Axon Res...	Active
12-072901	PHOTO 2020-07-29 10-101	SGT Schueler, David (10-...	SGT Schueler, ...	Jul 29, 2020 2:43 PM	Jul 29, 2020 10:41 AM	AI Training, Arrest, Ax...	Active
12-072901	AUDIO 2020-07-20 10-101	SGT Schueler, David (10-...	SGT Schueler, ...	Jul 29, 2020 2:43 PM	Jul 20, 2020 3:33 PM	1s	AI Training, Arrest, Ax...

The Review Mode viewer opens with all the selected evidence shown in the left-hand navigation panel.

Note: If you do not have permission to view a piece of evidence (such as restricted evidence or lack of permission), that evidence will not be visible in Review Mode.

3. Cycle through the evidence. While in Review mode you can:



- Click the link to go to the Evidence Detail Page for the evidence.

- Play videos and audio,
- Review and edit evidence description and metadata,

To edit evidence description or metadata; click the edit icon (✎) for the appropriate field, enter the information, and click **Save**.

- Add and edit Custom Metadata

Note: The ability to add and edit Custom Metadata fields in Review Mode is controlled by your Axon Evidence administrator. Contact them for questions about fields not being available in Review Mode.

To add Custom Metadata; under the Custom Metadata heading click **Add**, select a custom metadata field, add or select the information, and click **Save**.

To edit Custom Metadata; click the edit icon (✎), enter or select the information, and click **Save**.

- Add and edit Categories and Tags.

To add or edit Categories and Tags; click the edit icon (✎), select the category or tag, and click **Save**.

To remove a Category or Tags; click the edit icon (✎), click the **X** adjacent to the category or tag, and click **Save**.

- Add notes.

To add notes, enter the information in the Notes field and click **Add Note**.

4. When you are done reviewing and editing the evidence files, click **X** to close Review Mode.

Evidence Access Control Overview

Axon Evidence uses access classes to control access to evidence. Each piece of evidence in Axon Evidence is assigned to one of the following access classes:

- Unrestricted
- Restricted
- Confidential

Evidence can only be assigned to one access class at a time. Evidence normally enters Axon Evidence with the Unrestricted access class. The access class can be changed to Restricted or Confidential manually, by assigning the evidence to a Restricted or Confidential category, or by adding it to a Restricted or Confidential case.

Note: There are no Axon Evidence specific definitions for the Restricted and Confidential access classes. Your organization should determine how these classes are used within your organization.

User Access to Evidence and User Permissions

Default access to evidence is based on the permissions for a user's assigned role. The role-based permissions affect a user's ability to search for, view, and change the access class for evidence.

Additionally, each piece of evidence has its own access list, which allows your organization to manage evidence access inside and outside your organization on an as needed basis. Users and groups inside your organization can be granted access to evidence by being added to the access list. The access list is additive to role-based access. So, both users with role-based access and users on the access list are granted permission to search for and view the evidence. Being added to an access list allows a user to access the evidence, but it does not grant them any additional permissions beyond what is already included in their role.

See [Providing Access to Evidence Outside Your Organization](#) for information on managing access outside your agency.

The following table provides information on a user's ability to search for, view, and change the access class for evidence for the different permission settings.

Permission	Setting	Role-Based Access		Access List Member
		User	Group Monitor	
List Unrestricted Evidence List Restricted Evidence List Confidential Evidence	Prohibited	No evidence	No evidence	Can search and run reports if on the evidence access list
Sets permission to search for evidence and include evidence in reports evidence for the set access class.	Only Their Own	If assigned as evidence owner	If evidence owned by group member	Can search and run reports if on the evidence access list
	Any Evidence	Any evidence	Any evidence	Can search and run reports if on the evidence access list

Permission	Setting	Role-Based Access		Access List Member
		User	Group Monitor	
View Unrestricted Evidence View Restricted Evidence View Confidential Evidence Sets permission to access evidence for the set access class	Prohibited	No evidence	No evidence	Can view evidence if on the access list and granted View Only access.
	Only Their Own	If assigned as evidence owner	If evidence owned by group member	Can view evidence if on the access list
	Their Groups' & Their Own	If assigned as evidence owner or if evidence is assigned to a group the user is a member or monitor of	If evidence owned by group member	Can view evidence if on the access list
	Any Evidence	Any evidence	Any evidence	Can view evidence if on the access list
Apply Access Class - Restricted Apply Access Class - Confidential Sets permission to apply the access class	Prohibited	Cannot apply access class	Cannot apply access class	No effect
	Only Their Own	If assigned as evidence owner	If evidence owned by group member	No effect
	Their Groups' & Their Own	If assigned as evidence owner or if evidence is assigned to a group the user is a member or monitor of	If evidence owned by group member	No effect
	Any Evidence	Any evidence	Any evidence	No effect
Remove Access Class - Restricted Remove Access Class - Confidential	Prohibited	Cannot remove access class	Cannot remove access class	No effect
	Only Their Own	If assigned as evidence owner	If evidence owned by group member	No effect

Permission	Setting	Role-Based Access		Access List Member
		User	Group Monitor	
Sets permission to remove the access class	Their Groups' & Their Own	If assigned as evidence owner or if evidence is assigned to a group the user is a member or monitor of	If evidence owned by group member	No effect
	Any Evidence	Any evidence	Any evidence	No effect

Evidence Search Page Views

The information shown to users on the Evidence Search page and in reports depends on the permissions for the user's assigned role and if the user has been added to an access list. If a user does not have list permission for an access class and is not on the access list for evidence in that access class, then no evidence in that access class is shown on the Evidence Search page or in reports.

Example: If a user's assigned role has the List Unrestricted Evidence permission set to Only Their Own and the user is not on any access lists, then the user will not see any evidence that is in the Restricted or Confidential access class on the Evidence Search page.

If a user has list permission for an access class set to Only Their Own, then the user will only see the evidence they are assigned as the owner.

If the user has list permission for an access class set to Any Evidence and has view permission set to Only Their Own, then the user will see all the evidence in that access class but only be able view their own evidence. The user can request access to other evidence, as shown in the following image.

The screenshot shows the Axon Evidence search interface. At the top, there is a navigation bar with tabs: EVIDENCE, RECORDS, ALPR, CASES, INVENTORY, ADMIN, and HELP. Below this is a sub-navigation bar with: ALL EVIDENCE, MY EVIDENCE, SHARED EVIDENCE, and EVIDENCE MAP. The main search area includes fields for ID, TITLE, USER OR GROUP, DATE (with Start and End date pickers), CATEGORY, and TAG. There is also a CUSTOM METADATA field and a SHOW ADVANCED SEARCH link. A RESET FILTERS button and a SEARCH button are also present. Below the search area, the results are displayed as a table with columns: ID, TITLE, OWNER, UPLOADED BY, UPLOADED ON, RECORDED ON, CATEGORY, and STATUS. The table shows 84,500 results. A sample of the data is as follows:

ID	TITLE	OWNER	UPLOADED BY	UPLOADED ON	RECORDED ON	CATEGORY	STATUS
dd	pdinh test eeee	Griffith, Jason (23-414)	Sgt Dinh, Phuo...	Jun 12, 2020 2:32 PM	Jan 30, 2099 9:03 PM	Unknown	Request Access
ergrg	(Clip 2.1) (Extraction 4.1) (Clip ...	Le, Anh (12-333)	Le, Anh (12-333)	Mar 3, 2021 4:45 PM	Jan 30, 2099 9:03 PM	Unknown	Request Access
multi_coach	(Extraction 4.1) (Clip 2.1) pdinh...	Smith, Amy (23-456)	Nguyen, Luu (2...	Dec 3, 2020 10:30 PM	Jan 30, 2099 9:03 PM	Unknown	Request Access
ergrg	(Clip 1.1) (Clip 1.1) (Extraction ...	Dr Colosky, Edward (12-6...	Dr Colosky, Ed...	Mar 9, 2021 12:11 PM	Jan 30, 2099 9:03 PM	Unknown	Request Access
ergrg	(Extraction 1.1) (Clip 1.1) (Clip ...	Nguyen, Luu (22-222)	Nguyen, Luu (2...	Feb 25, 2021 1:14 AM	Jan 30, 2099 9:03 PM	Unknown	Request Access

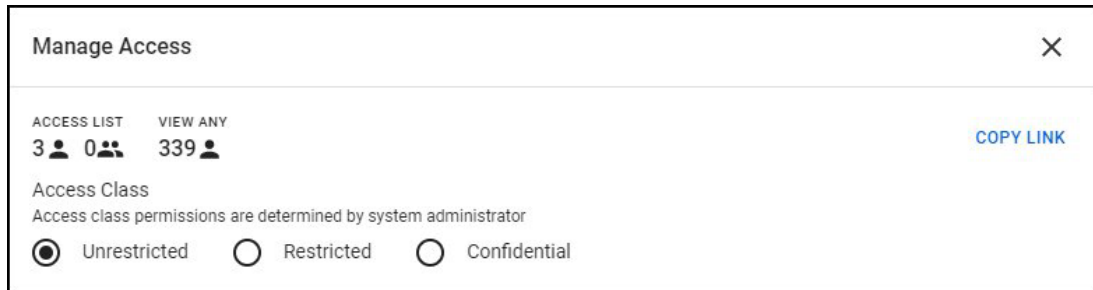
Access List Information

You can get a snapshot view of the number of users that can access an evidence file by looking at the manage access section of the Evidence Detail page. The following image shows that 342 role-based users and users that were added to the access list inside your organization have access to the evidence. Note that Group Monitors and Evidence Groups users are not included in the count. Additionally, this evidence has been shared with 1 agency outside your organization.

The screenshot shows the Axon Evidence Manage Access screen for a video file titled "VIDEO 2020-07-29 10-101". The ID is 07-004525. The categories are Axon Research and 6 months. The screen is divided into three main sections: DOWNLOAD, FLAG, and AUDIT TRAIL. The AUDIT TRAIL section shows a video thumbnail. On the right side, there is a "Manage Access" section with a green border. It shows "342" users inside the agency and "1" share outside the agency. Below this, there is a "Manage Shares" section with a "SHARE" button. At the bottom, there is a "No location added" section with a location picker icon. The bottom of the screen shows a "METADATA" section with an "ASSIGNED TO:" field.

A detailed view of user access can be found by clicking **Manage Access** to view the Manage Access screen for the evidence. The upper portion of the Manage Access screen shows the

number of users and groups on the access list, the number of users that can view the evidence due to their role-based permissions, and the access class for the evidence. The upper portion of the page also includes the link to the evidence page, allowing users to easily copy the link so it can be pasted into reports, documents, and other applications. Note that anyone using the link must still sign into their Axon Evidence account and must either be on the access list or have permission to view the evidence.



The screenshot shows the 'Manage Access' interface. At the top, there's a title bar with 'Manage Access' and a close button (X). Below this, there are two sections: 'ACCESS LIST' and 'VIEW ANY'. The 'ACCESS LIST' section shows '3' users and '0' groups. The 'VIEW ANY' section shows '339' users. To the right of these sections is a 'COPY LINK' button. Below these sections is the 'Access Class' section, which states 'Access class permissions are determined by system administrator'. There are three radio buttons for 'Unrestricted' (selected), 'Restricted', and 'Confidential'.

The Manage Access screen is also used to add and remove users and groups from the evidence access list and to change the evidence access class. Users must have the appropriate permission to apply or remove an access class. The lower portion of the Manage Access screen shows the users and groups on the access list for the evidence. The list shows the user or group name, access level, evidence access duration, and when the user or group was added to the list. If the evidence is in the restricted or confidential access class, then only users in roles that grant them access to evidence in the restricted or confidential access class and the users and groups on the access list can view the evidence.

Providing Access to Evidence Outside Your Organization

A detailed view of access outside your organization can be found by clicking **Manage Shares - Outside My Agency** to view the Manage Shares screen for the evidence.

Users with the appropriate permissions can provide access to the evidence for partner agencies and users outside your organization using the Manage Shares screen. Additionally, users can provide access to evidence using an unauthenticated download Link from the evidence search page.

The Manage Shares option does not provide a copy of the evidence to the partner agency. This is unlike sharing evidence by case to partner agency, which does provide a copy of the evidence and allows the agency to manage the video based on their own retention policies.

Access Classes and Categories

The Categories feature provides the ability to apply a Restricted or Confidential access class to evidence. When evidence is assigned to a category that applies an access class, the evidence access class is automatically changed. Because evidence can only have one access

class assigned at a time, if evidence is assigned to a Restricted category and to a Confidential category then the access class is changed to Confidential.

Note: If a user does not have permission to apply the Restricted or Confidential access class, then the user will not be able to assign evidence to a category that applies the access class change in Axon Evidence. Users applying categories using Axon mobile or desktop apps are not restricted from assigning categories.

Once an access class has been changed to Restricted or Confidential, it can only be changed to Unrestricted from the Evidence Detail page.

Changing Evidence Access Class

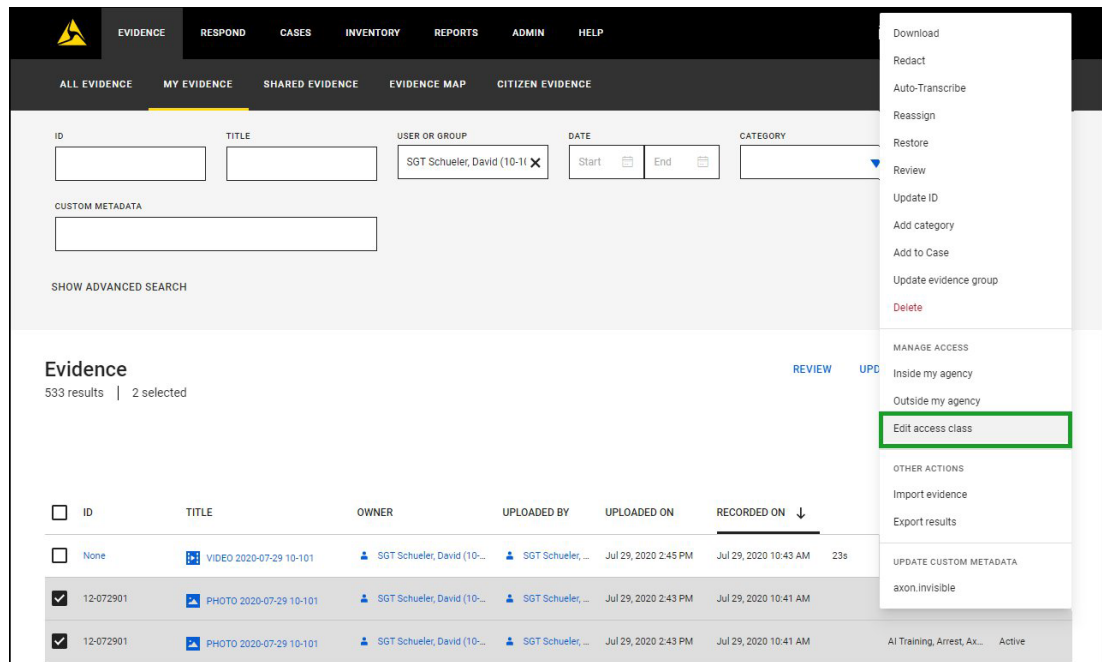
The access class for evidence can be changed by assigning a Restricted or Confidential category to the evidence or by manually changing the evidence access class. See [Add or edit Evidence Categories](#) for information on assigning a category to evidence.

Changing the access class of an evidence file only allows users that are on the evidence access list or that have list and view permissions for the access class to search for and view the evidence. Users that do not have list permission cannot see the evidence on the Evidence Search page.

Changing Evidence Access Class from the Evidence Search Page

From the evidence search page, you can change an access class and add users and groups to the access list for one or more evidence files 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 change.
3. Click the ... (More Action) menu and, under Manage Access, select **Edit Access Class**.



The Edit Access Class screen is shown on the right side of the page.

Note: The user that sets the evidence's access class to Restricted or Confidential will automatically be added to the access list.

4. Under Access Class, select **Restricted** or **Confidential**.

The 'Edit Access Class' dialog box is shown. It has a title bar with a close button (X). The main content area is divided into sections: 'Access Class' with radio buttons for Unrestricted (selected), Restricted, and Confidential; 'BULK OPTIONS' with radio buttons for Add to (selected) and Replace; 'ACCESS LEVEL' with a dropdown menu set to 'Role'; 'DURATION' with a dropdown menu set to 'Until Removed'; 'ADD ACCESS' with a text input field labeled 'Enter name, email address, or badge ID'; and a table with columns 'NAME' and 'MEMBERS'. The table shows one member: 'Schuer, David (10-101)'. At the bottom right are 'CANCEL' and 'SAVE' buttons.

5. Under Bulk Options, select how the access lists for the selected evidence files are affected:

- Select **Add to** to add the selected users or groups to the current access list.
- Select **Replace** 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.

6. 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.

7. 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 manually removed from the access list.

8. In the **Add Access** field, start typing the name, badge ID, or email address of the user or the name of the group. Axon Evidence 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) icon and then clicking **Remove**.

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

10. Click **Save**.

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

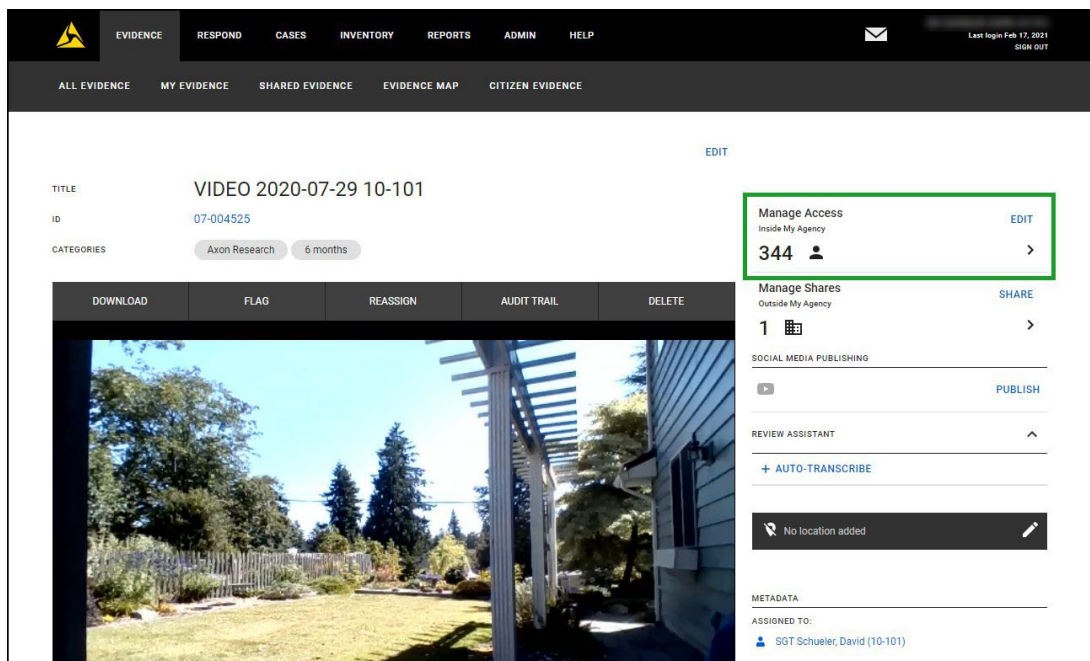
An email is sent to each user informing them that they have been added to the access list for the selected evidence files.

Note: If the Add to option was selected, an email is sent to users that were on the access list for this evidence informing them that the evidence was restricted, but that they still have access. If the Replace option was selected, an email is sent to users that were on the access list for this evidence informing them that they no longer have access to the evidence.

Changing Evidence Access Class from the Evidence Detail Page

From the Manage Access section you can add users and groups to the access list for an evidence file and change the evidence's access class. If you want to add users to the access list and change evidence access class for more than one evidence file at a time, use the process for [Changing Evidence Access Class from the Evidence Search Page](#).

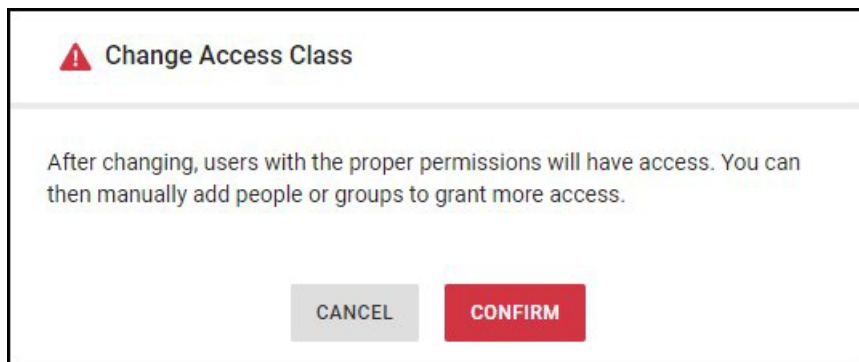
1. On the Evidence Detail page click **Manage Access**.



The Manage Access screen is shown on the right side of the page.

2. In the Access Class, select **Restricted** or **Confidential**.

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



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

Manage Access

ACCESS LIST VIEW ANY
1 0 298 Restricted COPY LINK

Access Class
Access class permissions are determined by system administrator
☐ Unrestricted ☒ Restricted ☐ Confidential

Add to access list

USER OR GROUP
Enter name, email address, or badge ID

NAME	MEMBERS	ACCESS TYPE	DURATION	ADDED ON
Schueler, David (10-101)		Manual	Until Removed	Oct 23, 2020

CANCEL DONE

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.

Manage Access [X]

ACCESS LIST: 1 user, 298 groups. [Restricted] [COPY LINK]

Access Class: Access class permissions are determined by system administrator.
☐ Unrestricted ☒ Restricted ☐ Confidential

Add to access list

USER OR GROUP: Enter name, email address, or badge ID

98-146 Dave Shoe [X]

[ADD]

ACCESS LEVEL: Role [v] DURATION: Until Removed [v]

NAME	MEMBERS ?	ACCESS TYPE	DURATION	ADDED ON
[User Icon] Schueler, David (10-101)		Manual	Until Removed	Oct 23, 2020 [Edit] [Delete]

[CANCEL] [DONE]

- 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 manually removed from the access list.

Manage Access

ACCESS LIST: 1 0 298 **Restricted** [COPY LINK](#)

Access Class
Access class permissions are determined by system administrator

☐ Unrestricted ☒ Restricted ☐ Confidential

Add to access list

USER OR GROUP: Enter name, email address, or badge ID

ACCESS LEVEL: Role

DURATION: **Until Removed**

98-146 Dave Shoe x

ADD

NAME	MEMBERS	ACCESS TYPE	DURATION	ADDED ON
Schueler, David (10-101)	Manual	Until Removed	Oct 23, 2020	

CANCEL **DONE**

- Click **Add**.

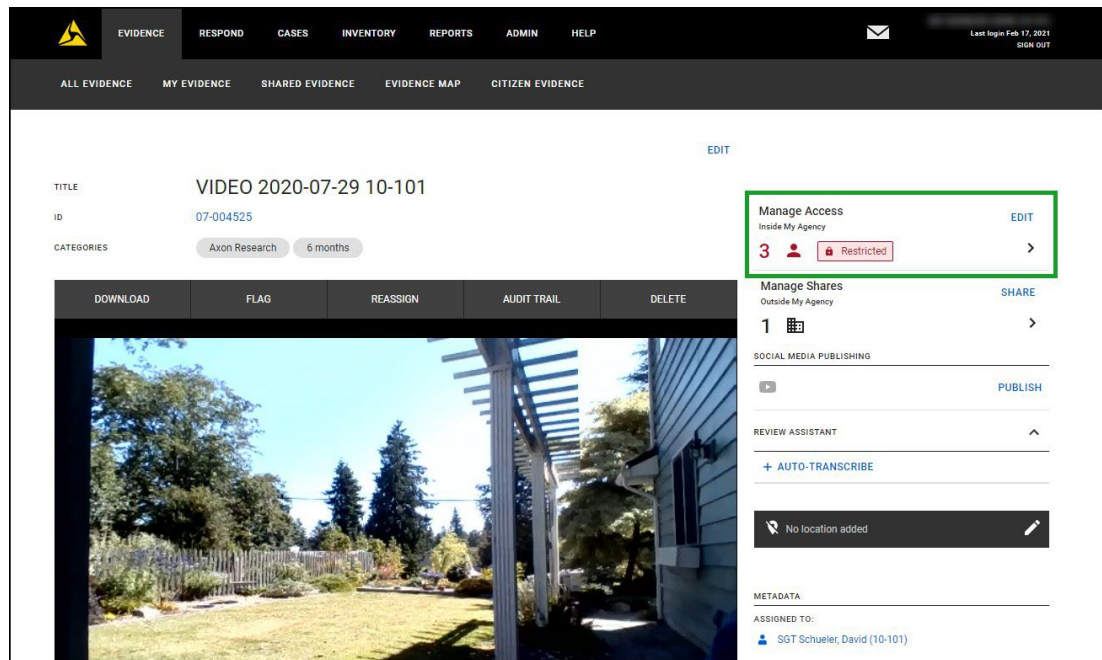
The user information is added to the list and an email is sent to the user informing them that they have been added to the access list for the evidence.

- Repeat steps 3 through 6 to add other users.
- After all users and groups are added, click **Done** to return to the Evidence Detail page.

Removing a Restricted or Confidential Access Class from Evidence

Evidence Restricted or Confidential access class can only be removed from the Evidence Detail page.

1. On the Evidence Detail page click **Manage Access**.



The Manage Access screen is shown on the right side of the page.

2. In the Access Class, select **Unrestricted**.
3. Click **Done** to return to the Evidence Detail page.

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.

Changing Evidence Access

Evidence access lists can be set from the Evidence Search and Evidence Detail pages.

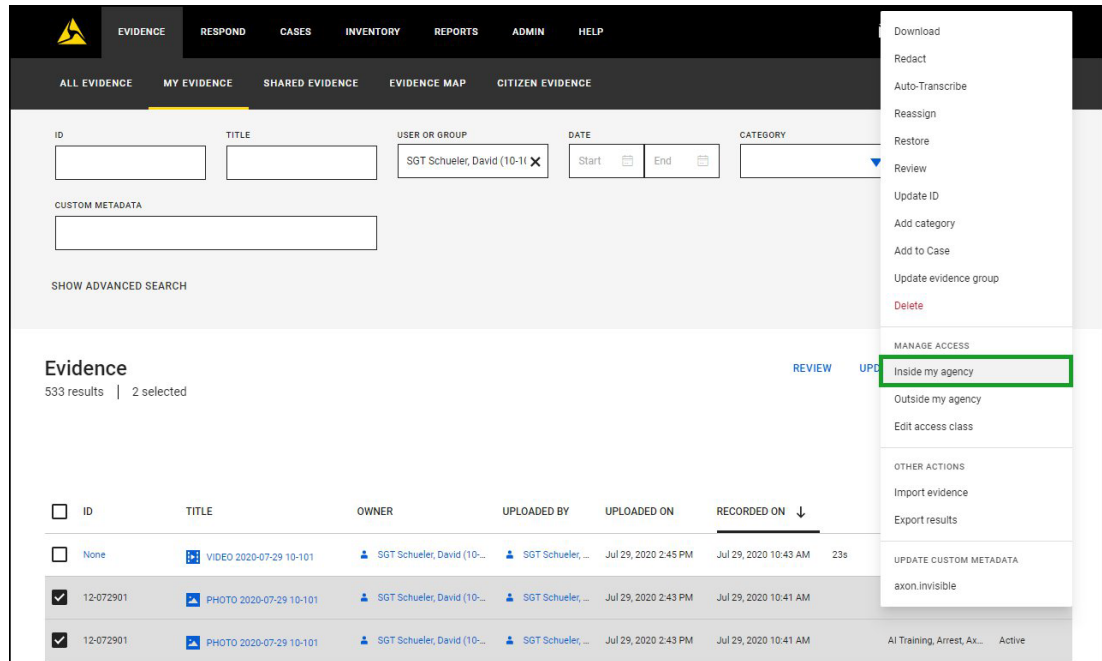
Adding Users and Groups to an Inside My Agency Access List from the Evidence Search Page

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 with a Restricted or Confidential access class.

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. Click the ... (more actions) menu and, under Manage Access, select **Inside My Agency**.



The Manage Access screen is shown on the right side of the page.

4. Under Bulk Options, select how the access lists for the selected evidence files are affected:

The screenshot shows the 'Manage Access' dialog box. It has a title bar with a close button (X). Inside, there are two sections: 'BULK OPTIONS' and 'ACCESS LEVEL'. The 'BULK OPTIONS' section has two radio buttons: 'Add to' (selected) and 'Replace'. The 'ACCESS LEVEL' section has two dropdown menus: 'Role' (set to 'Role') and 'DURATION' (set to 'Until Removed'). Below these is an 'ADD ACCESS' section with a text input field labeled 'Enter name, email address, or badge ID'. At the bottom of the dialog, there is a 'CANCEL' button and a 'SAVE' button.

- Select **Add to** to add the selected users or groups to the current access list.

- Select **Replace** 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.

5. 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.

6. 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 manually 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. Axon Evidence 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 **Save**.

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

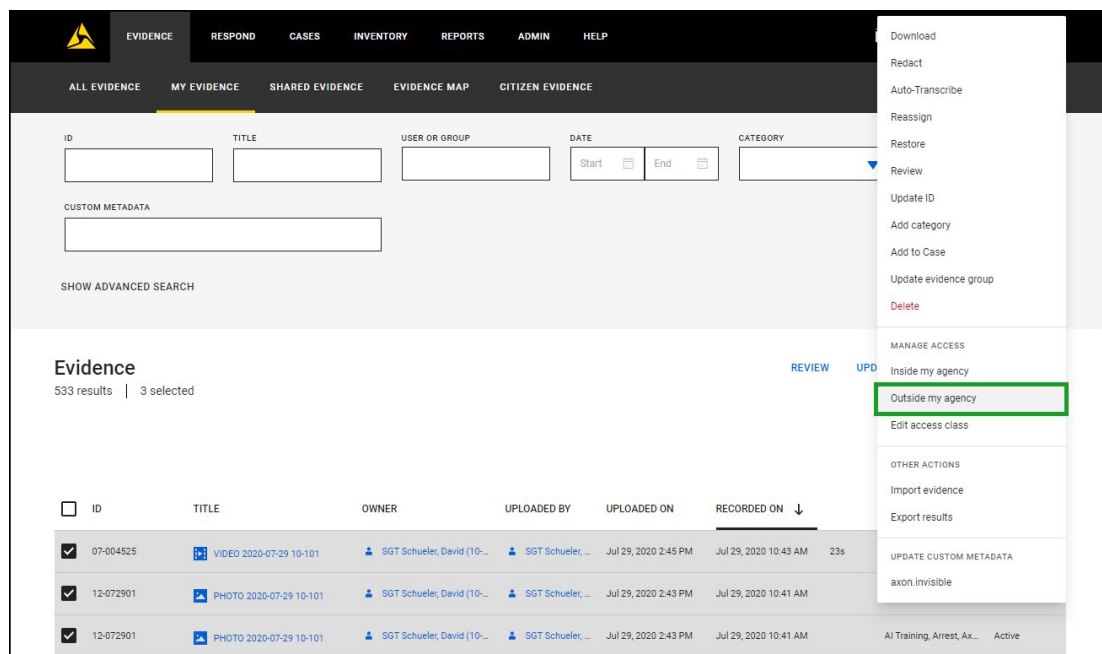
This option allows you to add users and groups to an external access list for multiple evidence files at the same time.

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 their own My Axon Evidence accounts. 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 Users and Groups on the Outside My Agency 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. Click the ... (more actions) menu and under Manage Access, select **Outside My Agency**.



The Share Outside My Agency screen is shown on the right side of the page.

4. Under Add Name to External Access List.

5. In the **Email** 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 Axon Evidence 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.

Note: If you add the email address for someone that is a member of an Axon Evidence agency that is not a partner agency with your agency, that person will be able to access the evidence when they sign in to their Axon Evidence agency. Users who are not part of an Axon Evidence agency can view the evidence through my.evidence.com.

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 **Reshare** option for the selected evidence.

- Never — User cannot share the evidence.

- Download — User can forward the permission to download to other users.
 - 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 **Share** and then, on the confirmation message box, click **Close**.

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

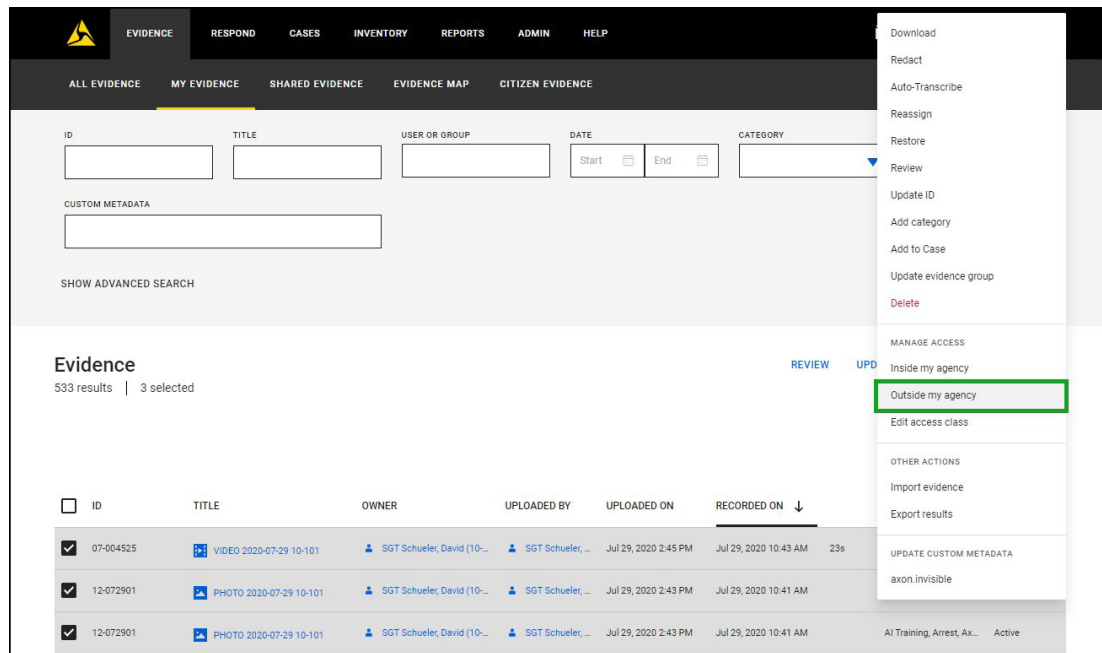
Providing Evidence Outside My Agency by Unauthenticated Download Link from the Evidence Search Page

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

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.

- Click the ... (more actions) menu and under Manage Access, select **Outside My Agency**.



The Share Outside My Agency screen is shown on the right side of the page.

- Click Email a Download Link.

The screenshot shows a modal dialog box titled 'Share Outside My Agency'. It has two tabs: 'ADD NAME TO EXTERNAL ACCESS LIST' and 'EMAIL A DOWNLOAD LINK' (which is selected and highlighted with a yellow underline). The 'EMAIL A DOWNLOAD LINK' tab contains the following fields:

- EMAIL:** A text input field with the placeholder text 'Enter Name, Email address, or Badge ID'.
- OPTIONAL MESSAGE:** A larger text area for an optional message.
- INCLUDE:** A section with three checkboxes: 'Audit Trails', 'Table of Contents', and 'Transcripts'.
- DURATION (DAYS):** A text input field with the value '3'.

 At the bottom of the dialog, there is a note: 'A link sent to the selected names will let them download a zip file for the given duration.' and two buttons: 'CANCEL' and 'SHARE'.

- In the **Email** 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 Axon Evidence 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.

6. If you want to include audit trails, a table of contents, and transcripts, check the corresponding check box.

When selected, the table of contents will accompany the bulk download as an Excel spreadsheet and includes the fields: File Name (with a link to the evidence file), Evidence ID, Evidence Title, File Type, File Size, Evidence Duration, Date Recorded, Uploader-First Name, Uploader-Last Name, Uploader-Badge ID, Assignee-First Name, Assignee-Last Name, Assignee-Badge ID, and Agency Name.

7. In the **Duration** box, type the number of days that the evidence is to be available to the users you share the evidence with.
8. Click **Share**.
9. On the notification message box, click **Close**.

Each recipient you specified receives an email that includes the link for downloading the evidence.

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

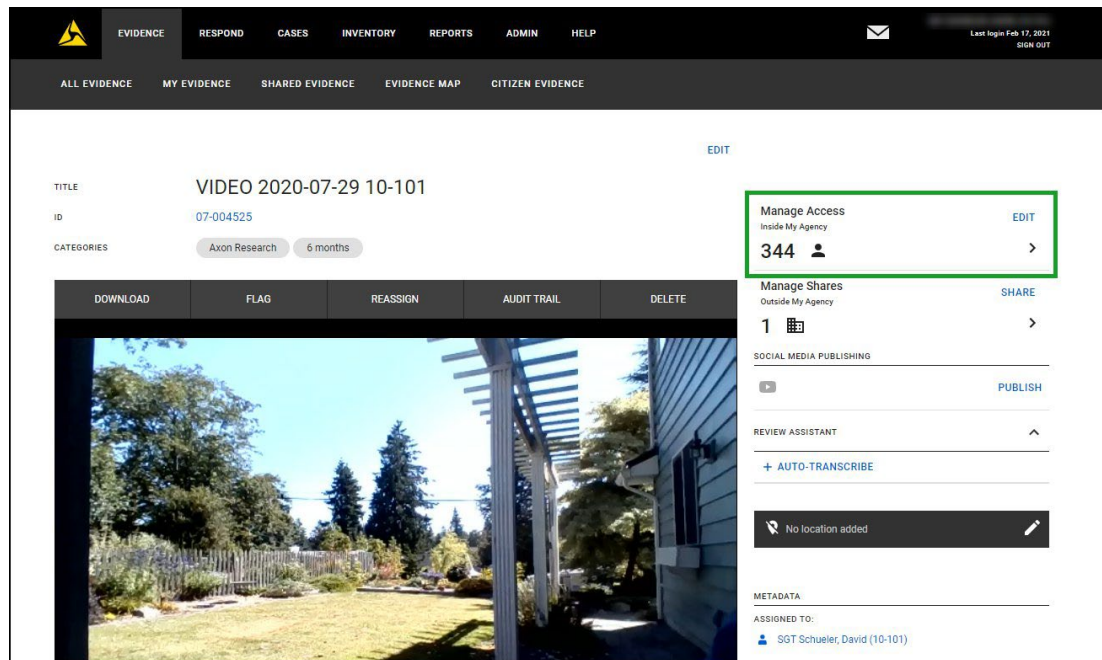
Adding Users and Groups to the Inside My Agency Access List from the Evidence Detail Page

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

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 Users and Groups to an Inside My Agency Access List from the Evidence Search Page](#).

Note: This procedure can also be used to add users and groups to the access list for evidence with a Restricted or Confidential access class.

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



The Manage Access screen is shown on the right side of the page.

2. Select the Access Class, **Unrestricted**, **Restricted**, or **Confidential** as needed.

The "Manage Access" dialog box is shown. It has a title bar with a close button. Inside, there are two tabs: "ACCESS LIST" and "VIEW ANY". Below the tabs, it shows "0" users and "342" groups. The "Access Class" section is highlighted with a green box, showing three radio buttons: "Unrestricted" (selected), "Restricted", and "Confidential". Below this is the "Add to access list" section. It has three fields: "USER OR GROUP" with a placeholder "Enter name, email address, or badge ID", "ACCESS L..." with a dropdown menu showing "Role", and "DURATION" with a dropdown menu showing "Until Removed". At the bottom, there are "CANCEL" and "DONE" buttons. A message at the bottom says "No users or groups have been added to the access list".

3. In the **User or Group** field, start typing the name, badge ID, or email address of the user or the name of the group. Axon Evidence 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.

Manage Access

ACCESS LIST 0 0 342 COPY LINK

Access Class
Access class permissions are determined by system administrator

☒ Unrestricted ☐ Restricted ☐ Confidential

Add to access list

USER OR GROUP
Enter name, email address, or badge ID

ACCESS L...
Role

DURATION
Until Removed

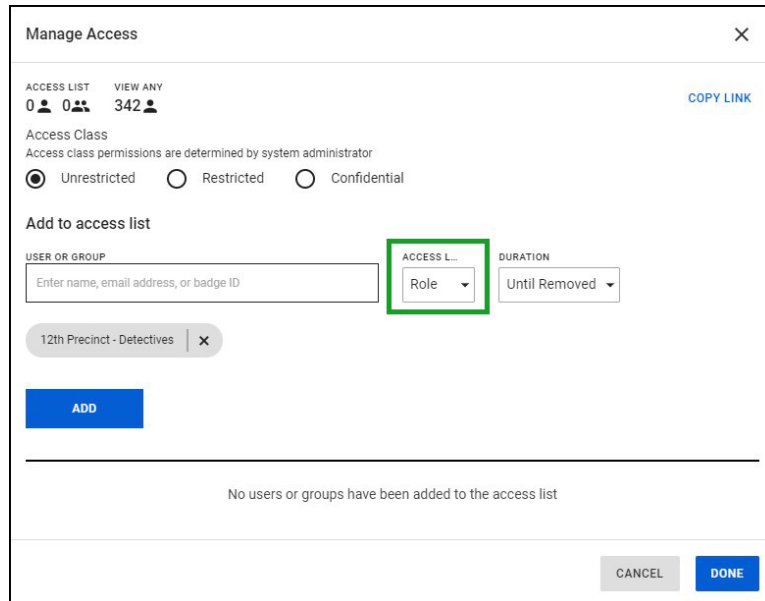
No users or groups have been added to the access list

CANCEL DONE

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.

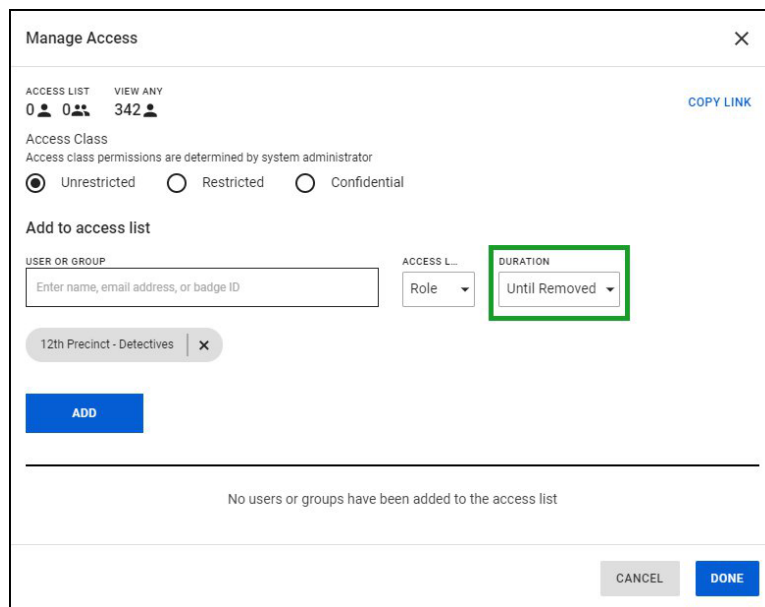
- If **Role** is selected, the actions a user can take with the evidence depends on the permissions associated with their assigned role.
- If **View Only** is selected, the user can only view the evidence.



The screenshot shows the 'Manage Access' dialog box. At the top, there's a title bar with a close button. Below it, the 'ACCESS LIST' section shows '0' users and '342' groups, with a 'COPY LINK' button. The 'Access Class' section has three radio buttons: 'Unrestricted' (selected), 'Restricted', and 'Confidential'. The 'Add to access list' section contains a text input for 'USER OR GROUP' with a placeholder 'Enter name, email address, or badge ID'. To its right is the 'ACCESS L...' dropdown, which is highlighted with a green box and shows 'Role' selected. Further right is the 'DURATION' dropdown, which shows 'Until Removed'. Below these is a tag '12th Precinct - Detectives' with a close button. At the bottom left is an 'ADD' button, and at the bottom right are 'CANCEL' and 'DONE' buttons. The main area of the dialog is empty, with a message 'No users or groups have been added to the access list'.

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 manually removed from the access list.



This screenshot is identical to the previous one, showing the 'Manage Access' dialog box. In this view, the 'DURATION' dropdown is highlighted with a green box and shows 'Until Removed' selected. The 'ACCESS L...' dropdown still shows 'Role'.

6. Click **Add**.

The user or group 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 2 through 6 to add other users and groups.

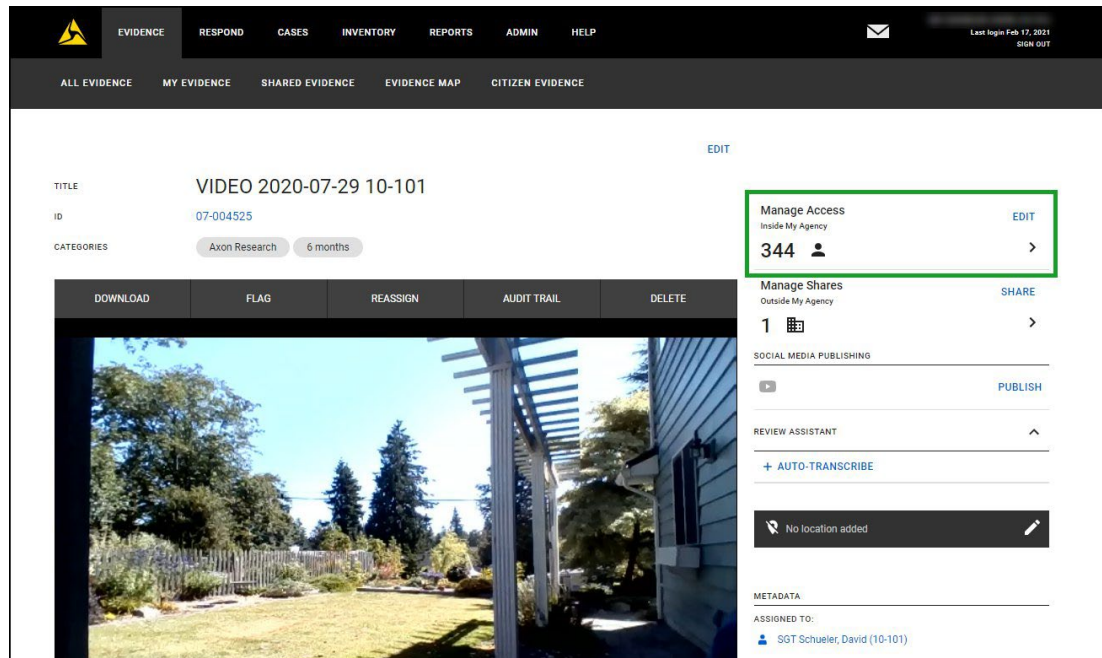
8. After all users are added, click **Done** to return to the Evidence Detail page.

Modifying an Inside My Agency Access List

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

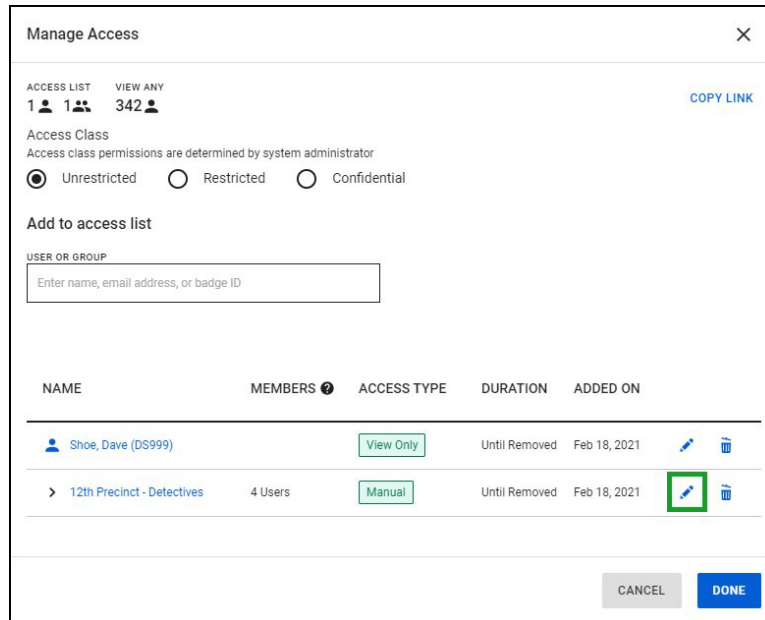
Note: This procedure can be used to modify access information for evidence with a Restricted or Confidential access class.

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



The Manage Access screen is shown on the right side of the page.

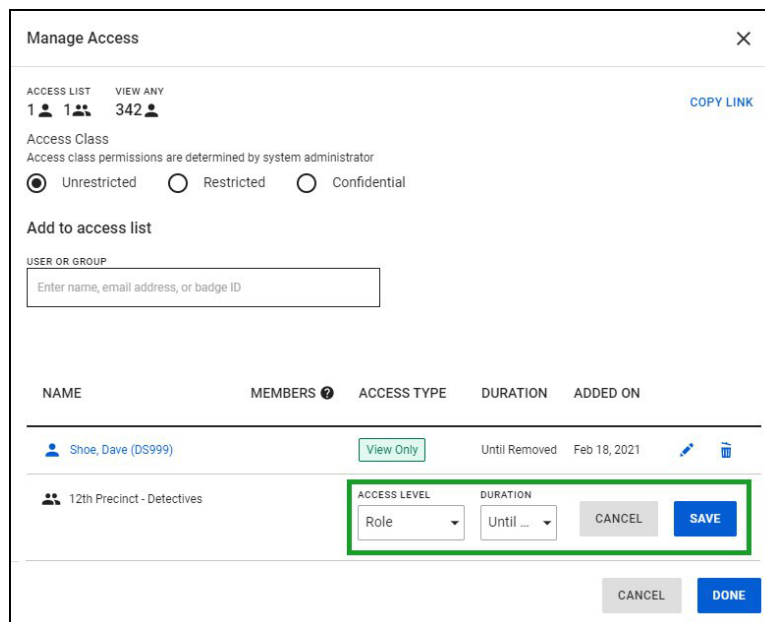
2. In the access list, click the edit icon on the same line as the user or group you want to modify.



The 'Manage Access' dialog box displays an 'ACCESS LIST' with two entries. The first entry is 'Shoe, Dave (DS999)' with a 'View Only' access type. The second entry is '12th Precinct - Detectives' with 4 users and a 'Manual' access type. The edit icon (pencil) for the second entry is highlighted with a green box. The dialog also includes an 'Access Class' section with radio buttons for 'Unrestricted', 'Restricted', and 'Confidential'. Below this is an 'Add to access list' section with a text input field for 'USER OR GROUP'. At the bottom are 'CANCEL' and 'DONE' buttons.

NAME	MEMBERS	ACCESS TYPE	DURATION	ADDED ON
Shoe, Dave (DS999)		View Only	Until Removed	Feb 18, 2021
> 12th Precinct - Detectives	4 Users	Manual	Until Removed	Feb 18, 2021

3. Select the access level and duration as needed.



The 'Manage Access' dialog box shows the edit form for the '12th Precinct - Detectives' entry. The 'ACCESS LEVEL' dropdown is set to 'Role' and the 'DURATION' dropdown is set to 'Until ...'. The 'SAVE' button is highlighted with a green box. The dialog also includes an 'Access Class' section with radio buttons for 'Unrestricted', 'Restricted', and 'Confidential'. Below this is an 'Add to access list' section with a text input field for 'USER OR GROUP'. At the bottom are 'CANCEL' and 'DONE' buttons.

NAME	MEMBERS	ACCESS TYPE	DURATION	ADDED ON
Shoe, Dave (DS999)		View Only	Until Removed	Feb 18, 2021
12th Precinct - Detectives		Role	Until ...	

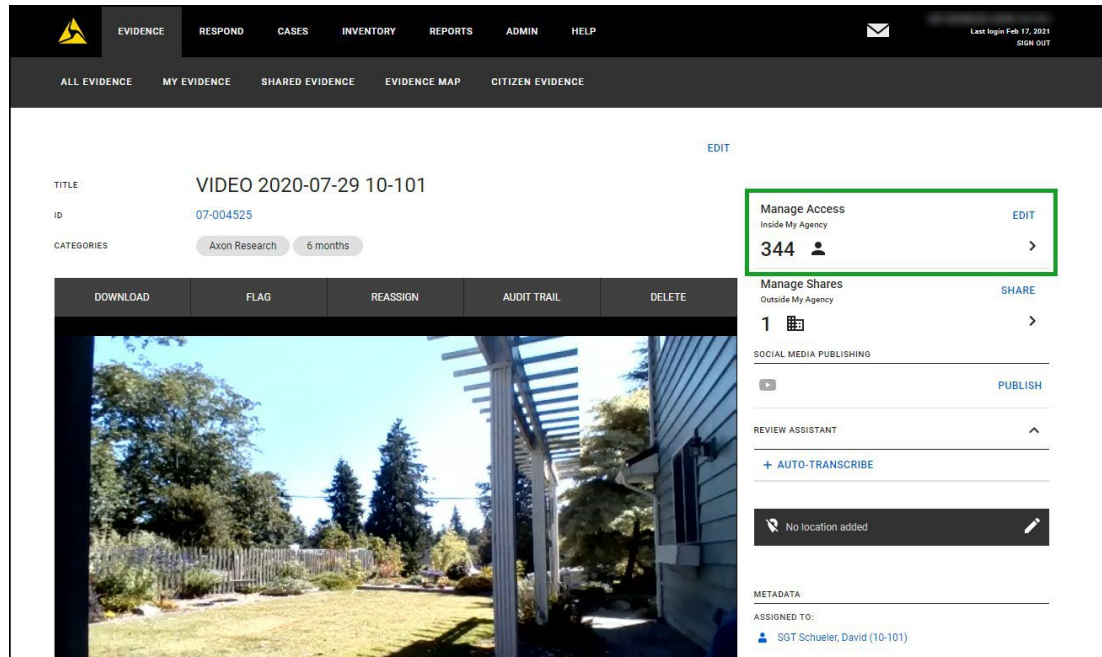
4. Click **Save**.
5. Repeat steps 2 through 4 for other users or groups in the list.
6. When you have finished modifying access information, click **Done** to return to the Evidence Detail page.

Removing Users and Groups from the Evidence 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 with a Restricted or Confidential access class.

1. On the Evidence Detail page, click **Manage Access**.



The Manage Access screen is shown on the right side of the page.

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

Manage Access

ACCESS LIST VIEW ANY
1 1 342 [COPY LINK](#)

Access Class
Access class permissions are determined by system administrator

☒ Unrestricted ☐ Restricted ☐ Confidential

Add to access list

USER OR GROUP
Enter name, email address, or badge ID

NAME	MEMBERS	ACCESS TYPE	DURATION	ADDED ON
Shoe, Dave (DS999)		View Only	Until Removed	Feb 18, 2021
> 12th Precinct - Detectives	4 Users	Manual	Until Removed	Feb 18, 2021

CANCEL DONE

The user or group 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.

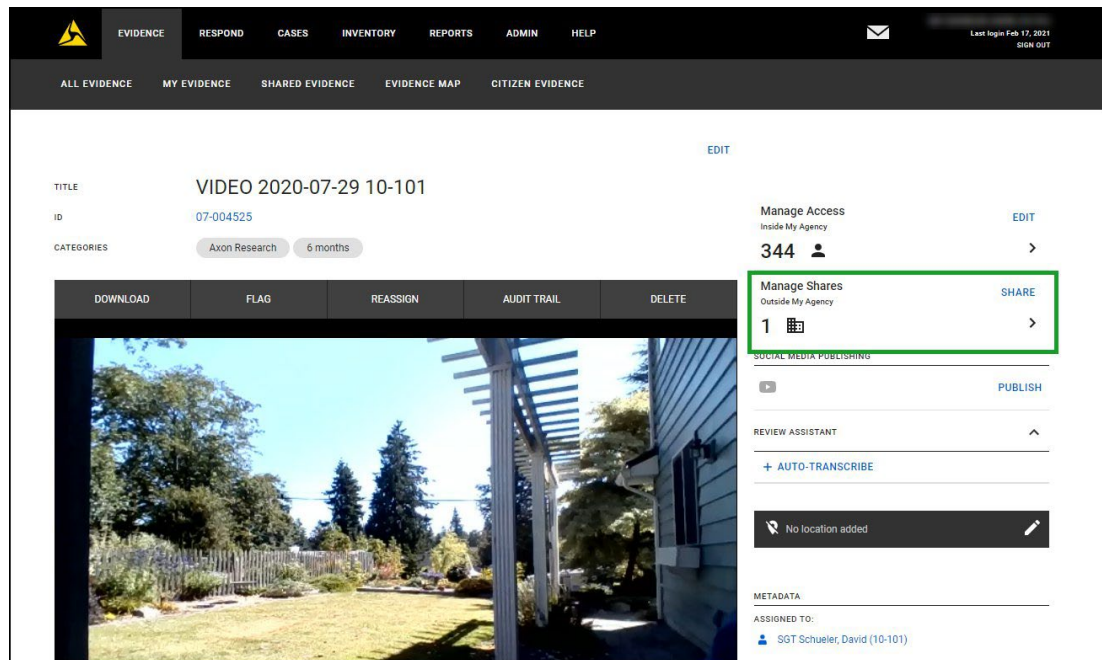
3. Repeat step 2 to remove other users and groups from the list.
4. When you have finished removing users, click **Done** to return to the Evidence Detail page.

Adding Users, Groups, and Agencies to the Outside My Agency Access List

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

From the Manage 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 Users and Groups to an Outside My Agency Access List from the Evidence Search Page](#).

1. On the Evidence Detail page, click **Manage Shares**.



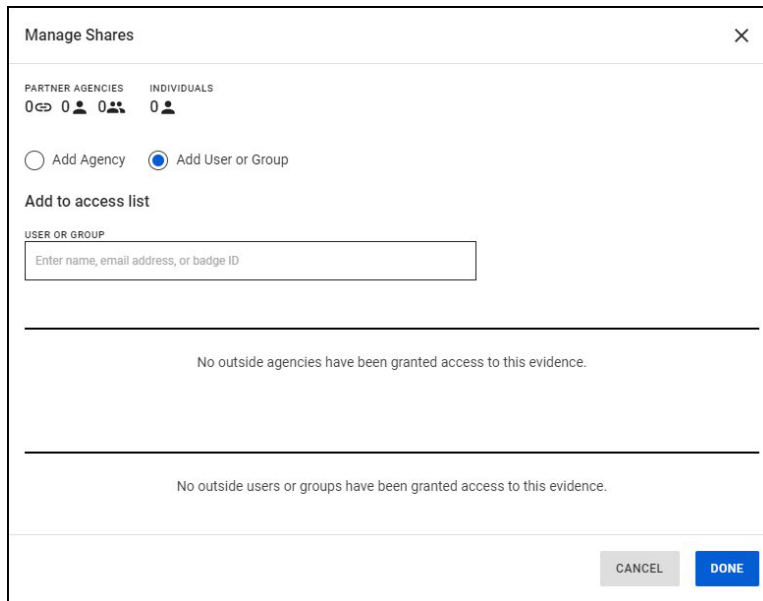
The Manage Shares screen is shown on the right side of the page.

2. To share with all users in a partner agency:

The "Manage Shares" dialog box is shown. It has a title bar with a close button (X). Inside, there are two sections: "PARTNER AGENCIES" and "INDIVIDUALS", both showing "0" users. Below these are radio buttons for "Add Agency" (selected) and "Add User or Group". A section titled "Add to access list" contains an "AGENCY" dropdown menu with the text "Select a partner agency". Below the dropdown, it states "No outside agencies have been granted access to this evidence." and "No outside users or groups have been granted access to this evidence." At the bottom right are "CANCEL" and "DONE" buttons.

- Select **Add Agency**.
- In the Agency field, start typing the agency name and select the agency you want to add to the access list.

- Click **Add**.
3. To share with specific users and groups in a partner agency:



The 'Manage Shares' dialog box is shown. It has a title bar with 'Manage Shares' and a close button. Below the title bar, there are two tabs: 'PARTNER AGENCIES' and 'INDIVIDUALS'. Under 'PARTNER AGENCIES', there are three icons representing different types of agencies. Under 'INDIVIDUALS', there is one icon representing an individual. Below the tabs, there are two radio buttons: 'Add Agency' (unselected) and 'Add User or Group' (selected). Below the radio buttons, there is a section titled 'Add to access list'. Under this section, there is a label 'USER OR GROUP' and a text input field with the placeholder text 'Enter name, email address, or badge ID'. Below the input field, there are two horizontal lines. The first line is followed by the text 'No outside agencies have been granted access to this evidence.' The second line is followed by the text 'No outside users or groups have been granted access to this evidence.' At the bottom right of the dialog box, there are two buttons: 'CANCEL' and 'DONE'.

- Select **Add User or Group**.
- In the **User or Group** field, start typing the name, badge ID, or email address of the user or the name of the group. Axon Evidence 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.

Note: If you add the email address for someone that is a member of an Axon Evidence agency that is not a partner agency with your agency, that person will be able to access the evidence when they sign in to their Axon Evidence agency. Users who are not part of an Axon Evidence agency can view the evidence through my.evidence.com.

- In the **Permissions** section, select the check boxes for the permissions that you want to give to the users you are sharing with.

- 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.
- Select the **Reshare** 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.

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

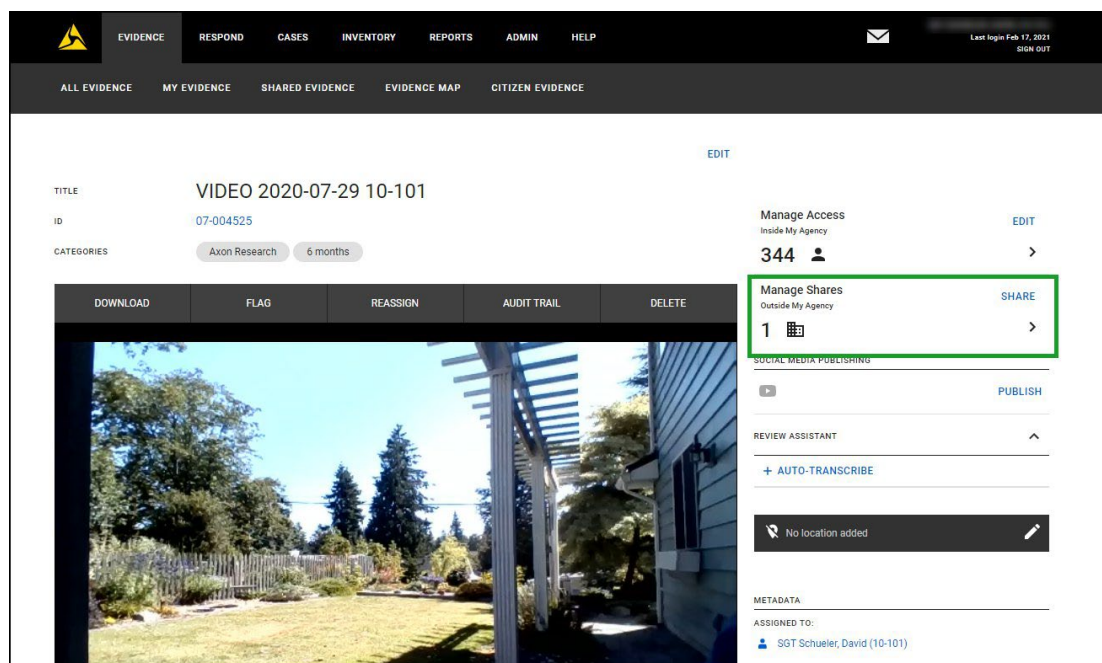
Axon Evidence emails each user who you shared the evidence with, notifying them that the evidence is available to them.

4. To add another agency or user or group with different permissions or duration, repeat the above steps.
5. After all agencies, users, and groups are added, click **Done** to return to the Evidence Detail page.

Modifying and Removing Users and Groups on the 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, click **Manage Shares**.



The Manage Shares screen is shown on the right side of the page.

2. To modify user or group information, click the edit icon on the same line as the user or group you want to modify.

Manage Shares

PARTNER AGENCIES

INDIVIDUALS

2

1

0

0

COPY LINK

☒ Add Agency

☐ Add User or Group

Add to access list

AGENCY

Evidence will be accessible by all users within the selected agencies.
Users given the link can view and download this evidence.

Select a partner agency

AGENCY

ADDED ON

Spurbury PD, sep24

Oct 23, 2020

NAME

MEMBERS

PERMISSIONS

RESHARE

DURATION

ADDED ON

Shoe, Dave (PER992)

View

Never

90 days rem...

Oct 23, 2020

CANCEL

DONE

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

Manage Shares [X]

PARTNER AGENCIES 2 1 0 INDIVIDUALS 0

[COPY LINK](#)

☒ Add Agency ☐ Add User or Group

Add to access list

AGENCY
Evidence will be accessible by all users within the selected agencies.
Users given the link can view and download this evidence.

Select a partner agency ▼

AGENCY	ADDED ON
Spurbury PD, sep24	Oct 23, 2020

NAME	MEMBERS ⓘ	PERMISSIONS	RESHARE	DURATION	ADDED ON
Shoe, Dave (PER992)		<div> PERMISSIONS <input checked="" type="checkbox"/> View <input type="checkbox"/> Download <input type="checkbox"/> View Audit <input type="checkbox"/> Add Notes </div>	<div> RESHARE Never ▼ </div>	<div> DURATION 90 </div>	

CANCEL SAVE

CANCEL DONE

3. Click **Save**.
4. Repeat steps 2 and 3 for other users or groups in the list.
5. To remove a partner agency, 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 partner agencies, users, or groups from the list.
7. When you have finished modifying access information, click **Done** to return to the Evidence Detail page.

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](#).

The screenshot displays the Axon Evidence Detail page for a video titled "4th and Main". The page layout includes a header with the title and ID (SB-5632), a row of action buttons (DOWNLOAD, FLAG, REASSIGN, AUDIT TRAIL, DELETE), and a large video player showing a busy city street scene. To the right of the video player, there is a "MANAGE EVIDENCE ACCESS" section with links for "INSIDE MY AGENCY" and "OUTSIDE MY AGENCY", both showing "None added". Below this is a "METADATA" section with the following details:

- Assigned To: Shoe, Dave (98146)
- Recorded On: Jan 18, 2018 8:45 AM -08:00
- Uploaded On: Feb 28, 2018 11:29 AM -08:00
- Uploaded By: Schuer, David (DS101)
- Deletion Scheduled For: Mar 19, 2020 9:45 AM -07:00
- File Size: 0.2 MB

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**.

<input type="checkbox"/>	ID	TITLE	OWNER	UPLOADED BY	UPLOADED ON	RECORDED ON ↓	CATEGORY	STATUS
<input type="checkbox"/>	45-5555	1	Menghani, Manish (187410...	Menghani, Manish (...)	21 Feb 2017 17:51:23	21 Feb 2017 17:48:41	Os	1.5 Year, 00000-Sha... Request Access
<input type="checkbox"/>	Add	AXON Body 2 Video 201...	Menghani, Manish (187410...	Menghani, Manish (...)	21 Feb 2017 17:40:18	21 Feb 2017 17:39:24	Os	00000-Shawn Request Access

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.

Bulk Update ID

You can change the ID assigned to one or more evidence files from the Evidence Search page. You can also [change the ID from the Evidence Detail page](#).

An evidence ID can be up to 75 alphanumeric characters, unless your administrator has configured evidence ID validation that enforces different minimum or maximum ID length.

1. Search for the evidence that 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** or click the ... (more actions) menu and select **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.

Bulk Add Categories to Evidence

You can add categories to one or more evidence files from the Evidence Search page. You can add or remove categories from the [Evidence Detail page](#).

Note: If a user does not have permission to apply the Restricted or Confidential access class, then the user will not be able to assign evidence to a category that applies the access class change in Axon Evidence. Users applying categories using Axon mobile or desktop apps are not restricted from assigning categories.

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** or click the ... (more actions) menu and select **Add Category**.

A dialog box appears.

4. In the New Category list, begin typing and then select click the category that you want to add to all selected evidence.
5. Click **Update**.
6. On the notification message box, click **Close**.

The search results show the category that you assigned to the evidence.

Bulk Add Tags to Evidence

You can add tags to one or more evidence files from the Evidence Search page. You can add or remove tags from the [Evidence Detail page](#).

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. A tag can be up to 256 alphanumeric characters.

1. Search for the evidence that you want to add tags to.
2. For each evidence file that you want to add tags to, select the check box to the left of the evidence.
3. Above the search results, click **Add Tag** or click the ... (more actions) menu and select **Add Tag**.

A dialog box appears.

4. In the Tag list, begin typing the tag name. Axon Evidence shows a list of existing tags that start with the typed letters. You can select an existing tag to apply by clicking it or finish typing the tag and click the **Create** option.
5. Click **Update**.
6. On the notification message box, click **Close**.

The tags are added to the 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. Click the ... (More Actions) menu and select **Reassign**.

The Reassign 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 and select the appropriate user.
5. Click **Reassign**.
6. 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.

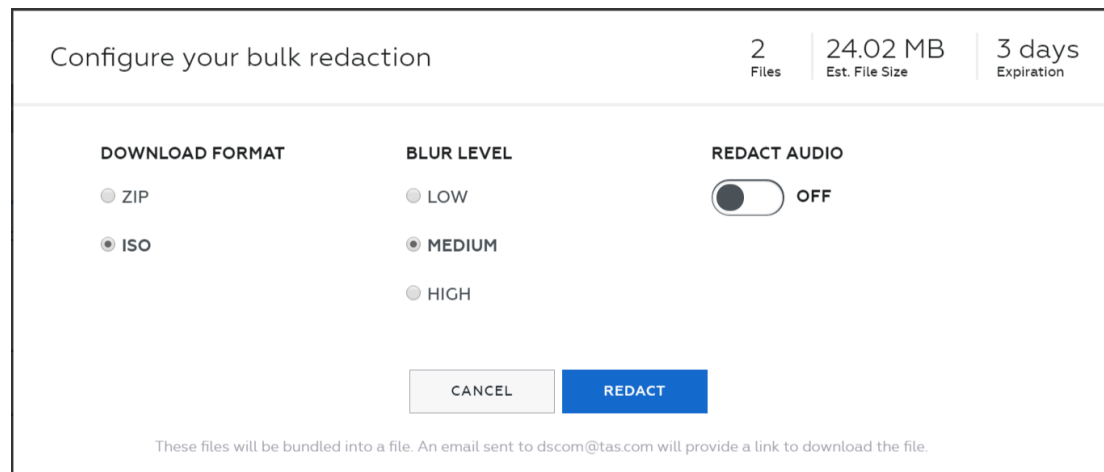
*Bulk redaction creates a copy of the original video and applies a blur filter over the **entire** copied video.* It can also remove audio for the duration of that copy as well. The blur over the entire video allows requestors to see what happened in the video without potentially revealing personally 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 the ... (More Action) menu and select **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.



The screenshot shows a dialog box titled "Configure your bulk redaction". In the top right corner, it displays "2 Files", "24.02 MB Est. File Size", and "3 days Expiration". The main area contains three sections: "DOWNLOAD FORMAT" with radio buttons for "ZIP" and "ISO" (where "ISO" is selected); "BLUR LEVEL" with radio buttons for "LOW", "MEDIUM" (selected), and "HIGH"; and "REDACT AUDIO" with a toggle switch currently set to "OFF". At the bottom, there are "CANCEL" and "REDACT" buttons. A small note at the very bottom states: "These files will be bundled into a file. An email sent to dscom@tas.com will provide a link to download the file."

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.

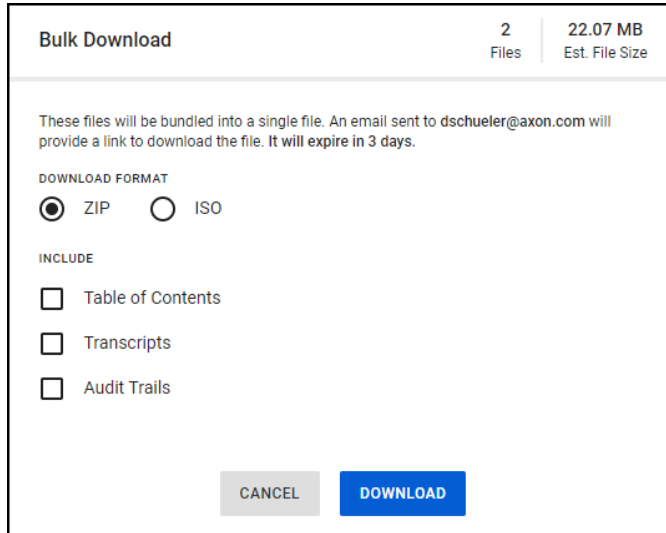
Bulk Download Evidence

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.
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 the ... (More Action) menu and select **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.

The image shows a 'Bulk Download' dialog box. At the top, it says 'Bulk Download' on the left, and '2 Files' and '22.07 MB Est. File Size' on the right. Below this, a message states: 'These files will be bundled into a single file. An email sent to dschueler@axon.com will provide a link to download the file. It will expire in 3 days.' Under the heading 'DOWNLOAD FORMAT', there are two radio buttons: 'ZIP' (which is selected) and 'ISO'. Under the heading 'INCLUDE', there are three checkboxes: 'Table of Contents', 'Transcripts', and 'Audit Trails', all of which are currently unchecked. At the bottom of the dialog box are two buttons: a grey 'CANCEL' button and a blue '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. If you want to include a table of contents file for the download, click the **Table of Contents** check box.

The table of contents will accompany the bulk download as an Excel spreadsheet and includes the fields: File Name (with a link to the evidence file), Evidence ID, Evidence Title, File Type, File Size, Evidence Duration, Date Recorded, Uploader-First Name, Uploader-Last Name, Uploader-Badge ID, Assignee-First Name, Assignee-Last Name, Assignee-Badge ID, and Agency Name.

7. 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.

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

A web browser opens your Evidence.com agency.

9. 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.

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

Approximate Download Speed					
File Size	24 Mbit/s	15 Mbit/s	10 Mbit/s	8 Mbit/s	2 Mbit/s
25 MB	10 seconds	13 seconds	20 seconds	30 seconds	1.75 minutes
50 MB	17 seconds	30 seconds	40 seconds	50 seconds	3.5 minutes
100 MB	30 seconds	1 minute	1.5 minutes	1.75 minutes	7 minutes
250 MB	1.5 minutes	2.5 minutes	3.5 minutes	4.5 minutes	17.5 minutes

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. Click the ... (More Action) menu and select **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.

Third-Party Video Support

The Third-Party Video Support feature allows users to playback videos that are not supported by the Axon Evidence default video player. When the feature is enabled and a third-party video is uploaded to Axon Evidence, the system will automatically start converting the file so that it can be viewed in Axon Evidence. The video in the original format is also maintained in the system.

Note: Third-Party Video Support is available in Axon Evidence for customers in the United States, the U.S. Federal region, Canada, Australia, and the United Kingdom. Third-Party Video Support for Europe, and Brazil is planned for 2021.

Files that are converted will show an informational message at the top of the video player to let the viewer know the video is not presented in its original format.

The screenshot displays the Axon Evidence web application. The top navigation bar includes links for EVIDENCE, RESPOND, CASES, INVENTORY, REPORTS, ADMIN, and HELP. The user is logged in as 'Last login 19 Oct 2020 10:04 AM'. The main content area shows details for a video titled 'Field_1_CCTV.dvt' with ID 4426 and category 'CCTV'. A red box highlights a message at the top of the video player: 'This video is not presented in its original file format.' The video player shows a soccer field. The right sidebar contains management options like 'Manage Access' (1038), 'Manage Shares' (0), and 'No location added'. Metadata includes 'ASSIGNED TO: Miller, JR (060123)', 'RECORDED ON: Oct 12, 2020 8:51 PM -07:00', 'UPLOADED ON: Oct 12, 2020 8:51 PM -07:00', 'UPLOADED BY: Miller, JR (060123)', 'DELETION SCHEDULED FOR: Unscheduled', 'FILE FORMAT: video/x-dvt', and 'FILE SIZE: 38.2 MB'.

Users can manually request conversion for files that were uploaded before the feature was enabled.

The screenshot displays the Axon Evidence web application. The top navigation bar includes links for EVIDENCE, RESPOND, CASES, INVENTORY, REPORTS, ADMIN, and HELP. The user is logged in as 'Last login 19 Oct 2020 10:04 AM'. The main content area shows details for a video titled '4k Sample3.g64' with ID 'None' and category 'Image Corrupted'. The video player area is black with a message: 'ADVANCED CODEC SUPPORT. It will take several minutes to prepare the evidence. An email will be sent to you when it is ready for review. REQUEST PLAYBACK'. The right sidebar contains management options like 'MANAGE EVIDENCE ACCESS' (1 INSIDE MY AGENCY, 0 OUTSIDE MY AGENCY), 'ASSIGNED TO: Schuer, David M (DS101)', 'RECORDED ON: May 2, 9999 9:38 AM -08:00', 'UPLOADED ON: Apr 15, 2020 1:38 AM -07:00', 'UPLOADED BY: Schuer, David M (DS101)', 'DELETION SCHEDULED FOR: Unscheduled', 'FILE FORMAT: video/x-g64', 'FILE SIZE: 58.5 MB', and 'EVIDENCE GROUP:'. There is also a 'CUSTOM METADATA' section with an 'ADD' button.

The feature will support the most common third-party file types. It will not support file types that are supported by the default video player (mp4, avi, etc.) but require a proprietary player/codecs for playback. We are working to expand support to include these file types as well.

For more information about enabling this feature for your agency, contact your Axon representative.

Metadata Overlays

Metadata overlays provide the ability for users to add evidence metadata onto video evidence while viewing the evidence and extract copies of the evidence with the metadata information embedded. This is accomplished by overlaying the metadata in the upper left section of the evidence display.

Metadata overlay functionality is available for Axon body-worn camera (BWC) videos, Axon Fleet videos, and converted third-party videos. Metadata overlays for multicam videos and other evidence types are not supported in the initial release.

The types of metadata that can be displayed and embedded depend on the type of evidence:

- **Axon BWC video:** Agency name, evidence ID, recorded on date and time, and Assigned To officer information.
- **Axon Fleet/Fleet 2 video:** Agency name, evidence ID, recorded on date and time, Assigned To officer information, and vehicle speed.
- **Axon Fleet 3 video:** Agency name, evidence ID, recorded on date and time, Assigned To officer information, vehicle speed, if the vehicle lightbar is on, if the vehicle siren is on, and if the vehicle brakes are being applied.

Note: Fleet videos that have two assigned officers will show the information for both officers.

- **Converted third-party video, non-Axon videos, and clips/extractions/redactions:** Agency name, evidence ID, recorded on date and time, and Assigned To officer information.

Your agency's Axon Evidence administrators can set which information is shown by default using [Evidence Playback Settings](#).

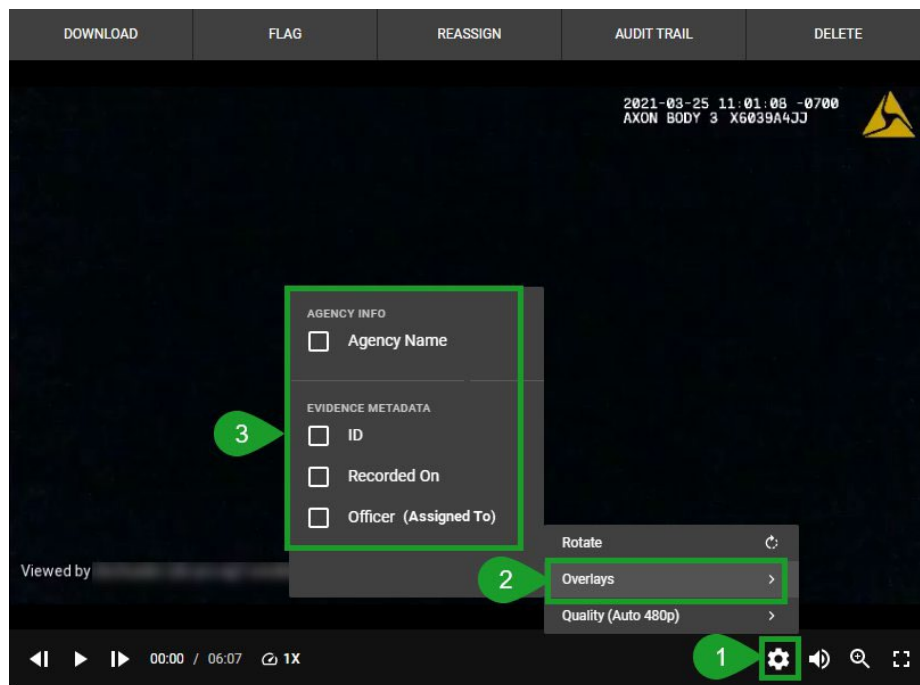
The agency name displayed is the same as name shown on the agency's Axon Evidence sign in page. The Assigned To officer information shown is set by your agency's Axon Evidence

administrators using Evidence Playback Settings and can be configured to show an officer's badge ID or first initial and last name or the first initial, last name, and badge ID.

Displaying Evidence Metadata with a Metadata Overlay

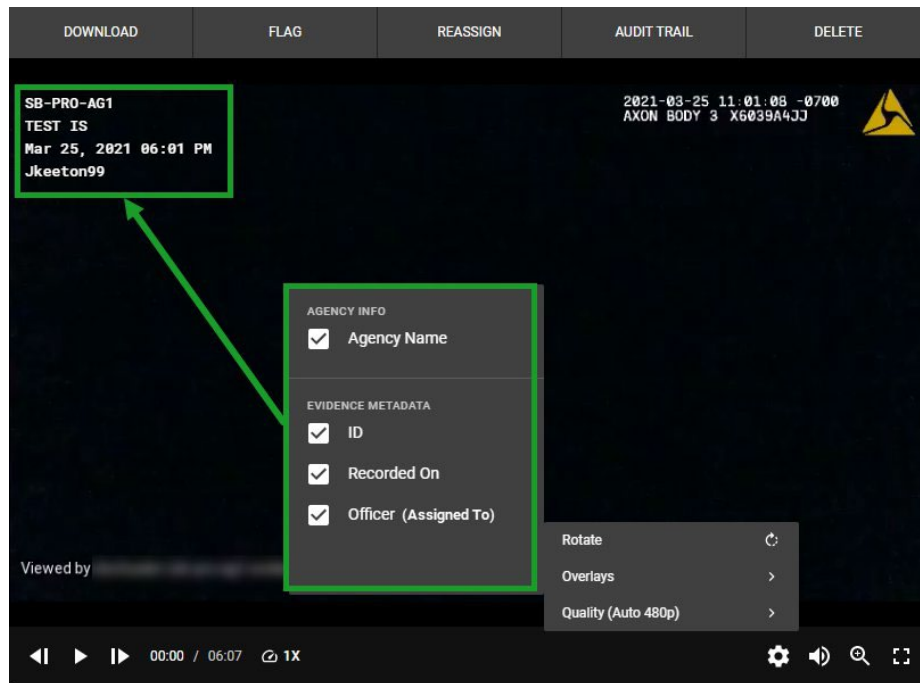
The metadata overlay information can be shown on evidence from the Evidence Detail page and while viewing evidence in Review Mode. Some overlays may be enabled by default. Check with your agency's Axon Evidence administrator for more information on which overlay information is shown by default.

1. To show the metadata, click the **More Settings** (gear) icon.
2. Select **Overlays**.
3. From the Overlays menu select the metadata options you want to view on the evidence.



Selecting a metadata option displays the information in the upper left of the evidence. The metadata is displayed in the same order, top to bottom, as is shown in the overlays

menu. If options that are higher on the list are not selected, the lower selected options are moved up the display list.

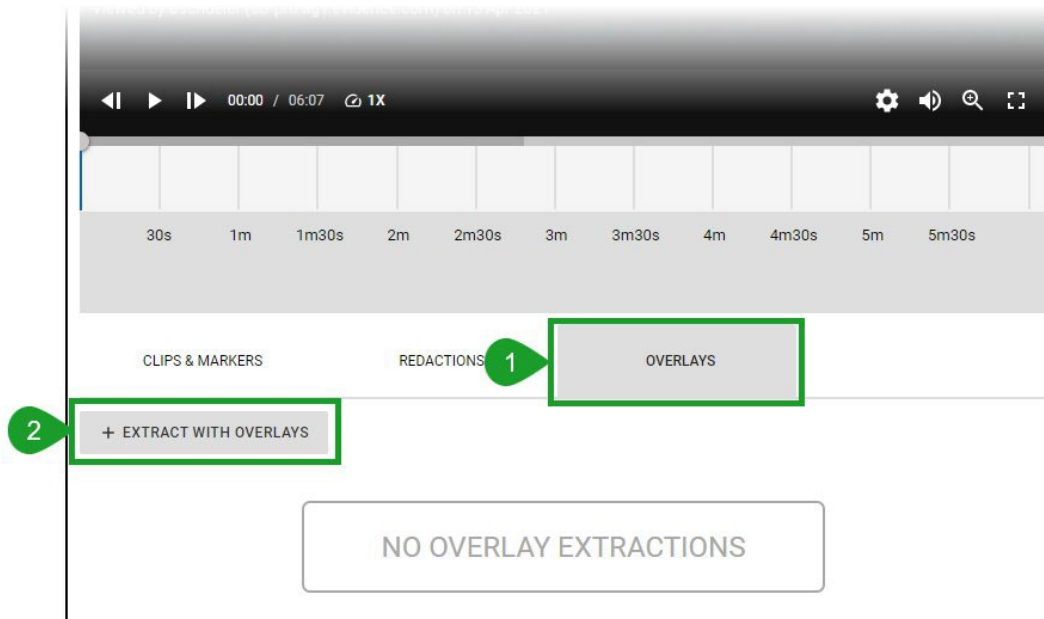


The information shown in the metadata overlay is only a preview. If the user leaves or refreshes the Review Mode or Evidence Detail page, the metadata is no longer shown when they return. To permanently embed the metadata, the user must extract a copy of the evidence while the metadata overlay is shown.

Extracting Evidence with a Metadata Overlay

Users with permission to edit the evidence can extract a copy of the evidence with the metadata overlays.

1. To create the extracted evidence, select the overlays you want to show in the evidence. Then click the **Overlays** tab under the evidence player.

2. Click **Extract with Overlays.**

Axon Evidence creates a copy of the evidence with the selected metadata overlays. The extraction is logged in the evidence audit trail and includes information about which metadata overlays were selected for the extraction.

Extracted evidence files can be used to create clips, redactions, and add markers.

Sharing Evidence and Metadata Overlays

The ability to use and view metadata overlay information in shared evidence files depends on how the evidence is shared.

- Manage Access Inside My Agency: Users added to the Internal Access Control List have access to the evidence and are able to review evidence with metadata overlays. Extraction with metadata overlays is controlled by user's permission to edit evidence.
- Manage Access Outside My Agency: Users added to the External Access Control List can view evidence with metadata overlays, but cannot create extractions.
- Manage Access Outside My Agency using a Download Link - The metadata overlays cannot be used during evidence playback. To share evidence with the metadata overlays, an extraction would need to be created and shared.
- Sharing Evidence through a Case - Metadata information included in the evidence is included when the evidence is shared in a case, but it is not displayed by default. When the original video is shared to a partner agency, all overlays available to the original agency will also be available to the partner agency. The only exception is the

Assigned To overlay, which gets a new value in the partner agency since the video assignment changes. In situations when only limited overlays should be available or when certain overlays must be embedded in a video, it is recommended that you create a video extraction with the overlays. Partner agencies are able to independently manage the extraction of videos with overlays.

When extracted evidence files are shared, the metadata overlays are visible to the viewer and cannot be changed.

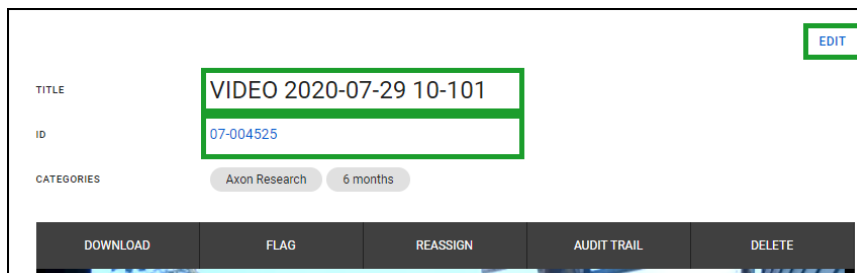
Edit Title and ID

On the Evidence Detail page, the evidence Title and ID appear above the evidence preview.

An evidence Title can be up to 200 alphanumeric characters.

An evidence ID can be up to 75 alphanumeric characters, unless your administrator has configured evidence ID validation that enforces different minimum or maximum ID length.

1. Click **Edit** or click the Title or ID field.



The Title, ID, and Categories fields become editable.

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

The Evidence Detail page shows the updated information.

Add or Edit Evidence Categories

You can add or remove categories from the Evidence Detail page. You can add categories to one or more evidence files from the [Evidence Search page](#).

Note: If a user does not have permission to apply the Restricted or Confidential access class, then the user will not be able to assign evidence to a category that applies the access class change in Axon Evidence. Users applying categories using Axon mobile or desktop apps are not restricted from assigning categories.

1. Click **Edit** or click the Categories field.

The Title, ID, and Category fields become editable.

2. To add a category, begin typing the category title in the Add Another field or use the down arrow to show the full list of categories, and then select the category.

3. To remove a category, click the **X** adjacent to the category name.
4. Repeat steps 2 and 3 to add or remove categories.
5. Click **Save**.

The Evidence Detail page shows the updated information.

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.

Action	Method
Directly edit the date and time.	Click the Recorded On box and enter the changes to the date and time.
Change the date.	Click the calendar icon and then use the calendar tool to select the date.
Change the time.	Click the clock icon and then select the closest time to the time that you need.

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).

- If you want to add the evidence to a case, in the **Enter Case ID** field, begin typing the ID for the case that you want to add the evidence to, select the case ID, and then click **Add to Case**.

The case that you selected appears under Associated Cases.

- If you want to remove the evidence from a case, find the case ID and then click **X**.
2. When you have finished adding or removing the evidence to and from cases, click **Cancel**.

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 dialog box appears.
2. 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 and select the appropriate user.
3. Click **Reassign**.
4. On the confirmation message box, click **Yes**.
5. On notification message box, click **OK**.

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 category's 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.

Extend a Retention Date

If evidence is assigned a category with a retention duration setting, you can extend the retention date for the evidence.

Note: Your assigned Role must have Category Administration permission to use the extend option.

The extend option will increase the retention date by the category's retention duration setting.

Example: If evidence is assigned to a category with a 1-year retention duration setting and a deletion date of February 13, 2019, extending the retention would change the deletion date to February 13, 2020.

On the Evidence Detail page for evidence, the Extend button appears above the evidence preview for users that have the correct permission.

1. Click **Extend**.
2. The confirmation message box asks you to confirm the extension and shows the new deletion date, click **Extend**.


The evidence retention date is updated.

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.

Note: If a user does not have permission to apply the Restricted or Confidential access class, then the user will not be able to assign evidence to a category that applies the access class change in Axon Evidence. Users applying categories using Axon mobile or desktop apps are not restricted from assigning categories.

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.

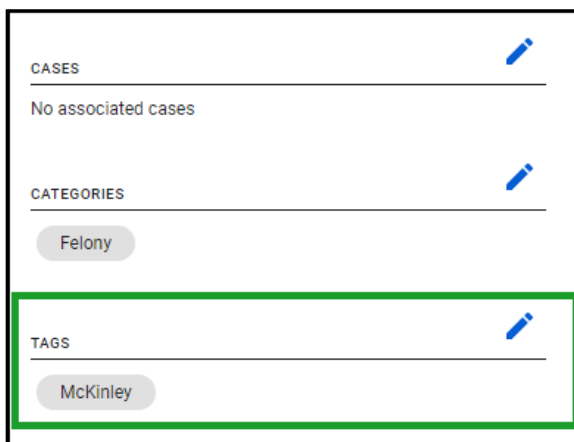
3. If you want to remove the evidence from a category, click the X next to the category.

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 below the Cases and Categories areas. If any tags exist, they appear as tiles. The following figure shows an example of the Tags area that has one tag named, "McKinley".



The screenshot displays the 'Evidence Detail' page interface. It is divided into three main sections: 'CASES', 'CATEGORIES', and 'TAGS'. The 'CASES' section at the top indicates 'No associated cases'. The 'CATEGORIES' section below it contains a single tag labeled 'Felony'. The 'TAGS' section at the bottom, which is highlighted with a green rectangular border, contains a single tag labeled 'McKinley'. Each of these three sections has a blue pencil icon in its top right corner, indicating an edit function.

A tag can be up to 256 alphanumeric characters.

1. In the **Tags** area, click the  (edit) icon.
2. To add a tag, start typing the tag information.

Axon Evidence shows you a list of existing tags that start with the letters you typed.

- If the tag you want to apply appears in the list, click the tag.
 - Otherwise, finish typing the tag and then press **Enter**.
3. To remove a tag, at the right side of tag name click the **X**.
 4. Add or remove additional tags as needed.

5. Click **Save**. Axon Evidence adds or removes the tags.

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.

ALSO WITH ID		
TITLE	ASSIGNED TO	CREATED ON
Backyard	MC Hamish	02/22/2016
Location of Fall -- East View	Bertram Brand	02/22/2016

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.

SOURCE	
Serial#:	x78002623
Model:	Axon Flex

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.

Axon Body 3 Camera Display and Notifications in the Field
The Axon Body 3 camera display, on top of the camera, shows information on camera status and activity. The camera also emits sounds called audio prompts to notify you of the device status or when you take an action. The audio prompts can be accompanied by a haptic notification (vibration) that matches the audio.

Operating Mode or Action	Camera Display (Activity Area)	Operation LED	Audio Notification	Haptic Notification (Vibration)
Power on	then READY	Solid red	Two short rising-pitch tones	One - long duration
Power off		Solid red	Three short lowering-pitch tones	One - long duration
Recording started by Event button double-press	STARTING then	Blinking red	Two short tones	Two - short duration
Recording started by Axon Signal		Blinking red	Two short tones	Two - short duration
Recording started by gunshot detection		Blinking red	Two short tones	Two - short duration
Recording reminder		Blinking red	Two short tones every 2 minutes	Two - short duration every 2 minutes
Stop recording, return to Ready	SAVING then READY	Blinking green	One long tone	One - long duration
Volume up or down		Blinking green or red	One short tone at new volume level	One - short duration
Connected for Axon Aware Live Streaming	LIVE	Blinking purple	Three short rising-pitch tones	One - long duration
Enter or Exit Mute mode (microphone off)		Blinking blue in Mute mode	One short tone	Two - long duration
Enter Stealth mode	STEALTH	Off	None	None
Exit Stealth mode	No change	Blinking green or red	None	Two - short duration
Event marker captured		Blinking red	None	One - short duration
Low battery notifications: 20% battery capacity and every 5% decrease OR any error	BATTERY LOW	Blinking yellow	Four quick high-pitch tones	Four - short duration
Camera enters Pairing mode	PAIRING	Blinking blue	Three short rising-pitch tones	None

Axon Body 3 Camera Display and Triad LED Status Information in the Dock
When you plug an Axon Body 3 camera into an Axon Body 3 Dock, the Triad LED on the front of the camera shows the device status and battery capacity. The Axon Body 3 camera display, on top of the camera, shows information on camera status and activity.

Device Status	Camera Display		Triad LED
	Activity Area	Status Bar	
Uploading data	UPLOADING 1/10		Spinning yellow (cycling on each Triad LED)
Downloading data or applying device settings	UPDATING		Spinning yellow (cycling on each Triad LED)
Applying firmware update - DO NOT remove camera from Axon Dock	UPDATING		Spinning white (cycling on each Triad LED)
Possible network error. Check network connection and refer to Troubleshooting section of the Axon Body 3 User Manual or go to help.axon.com .	NETWORK ERROR		Blinking red, yellow and green (cycling all colors)
Device error. Refer to device page in Axon Evidence.	NETWORK ERROR		Blinking red
Assign user ID - shown when no other activity (other than charging)	USERID123		Battery capacity
Battery capacity. The charge indicator is shown to the right of battery capacity during charge	Any of the above		Solid green (> 98%)
			Solid yellow (33% to 97%)
			Solid red (< 33%)

Play Store is a trademark of Google, Inc.; App Store is a trademark of Apple, Inc.
 ▲, ▲, ▲ AXON, Axon, Axon Body 3, Axon Dock, Axon View, and Axon Evidence are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information, visit www.axon.com/legal. All rights reserved. © 2019 Axon Enterprise, Inc. MPC0288 Rev B

1 - Search
2 - Page up and down
3 - Zoom
4 - Full screen

PDF Viewer Controls

1 - Search
(full screen only)



2 - Page up and down

3 - Zoom
(full screen only)

4 - Full screen

PDF Viewer Actions

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

Action	Steps
Search (full screen only)	Type text and numbers to search throughout the PDF file. The search functionality includes partial word searches but is not case sensitive. Note: The current search functionality does not support Optical Character Recognition (OCR) technology and will not recognize text inside images, such as from scanned documents and photos.
Page down	Click  or press the down arrow key.
Page up	Click  or press the up arrow key.
Zoom (full screen only)	
View Full Screen	To enter full-screen viewing mode, click the Full Screen icon. To exit full-screen viewing mode, press the ESC key.
View comments	You can view comments and notes by placing your cursor over notes and highlighted text.
Links	You can open external links and use internal links, such as table of contents links, to navigate through the PDF file.

Playing Video and Audio Evidence

This section describes the actions available on the Evidence Detail page for video and audio evidence files that are supported by the Axon Evidence media player.

Internet Connection Speed Recommendations

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

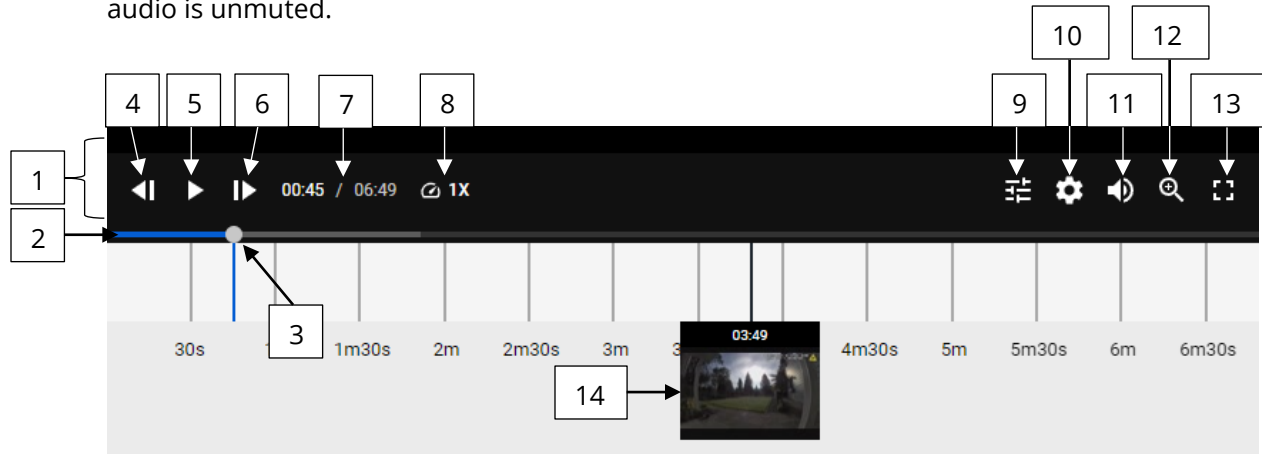
Resolution	Recommended Minimum Speed
480p	3 Megabits per second
720p	6 Megabits per second
1080p	10 Megabits per second

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

Media Player Controls

The Axon Evidence media player enables you to play audio and video evidence files that are in supported file types. Media player controls are provided below the media image.

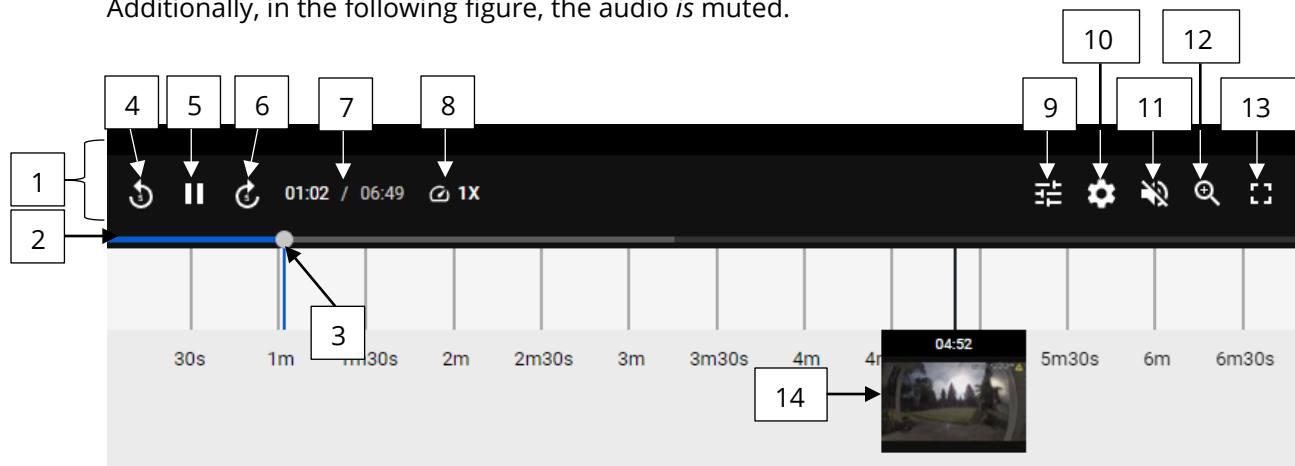
The following figure shows the basic media player controls while playback is paused, and the audio is unmuted.



Available Controls —Player Paused, Audio Unmuted

1 — Playbar	8 — Playback speed selector
2 — Scrub bar	9 — Brightness and contrast filters
3 — Scrub handle	10 — More settings (quality, overlays, rotate)
4 — Previous frame	11 — Mute/Volume control
5 — Play	12 — Zoom control
6 — Next frame	13 — Full screen
7 — Time information	14 — Thumbnail (shown on hover)

The following figure shows the media player controls that appear when the player is playing . Additionally, in the following figure, the audio is muted.

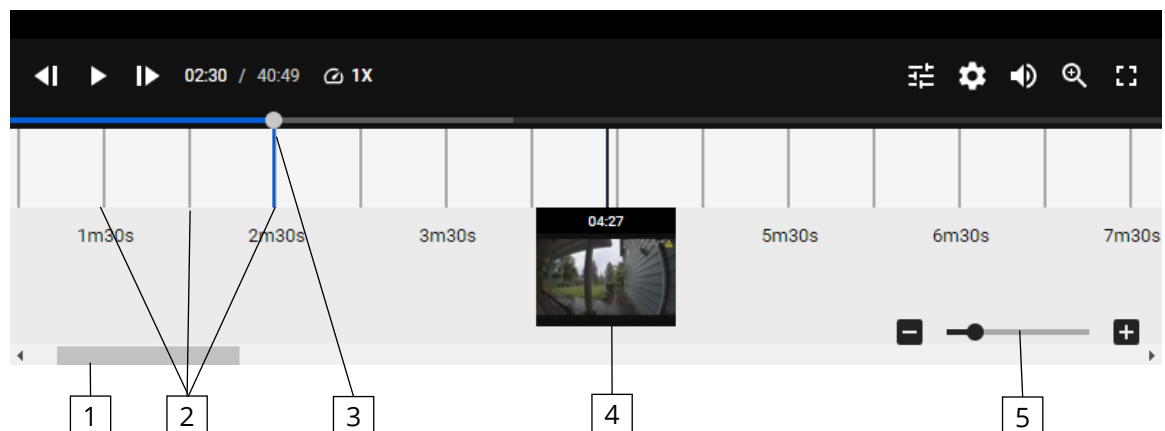


Available Controls —Player Playing, Sound Muted

1 — Playbar	8 — Playback speed selector
2 — Scrub bar	9 — Brightness and contrast filters
3 — Scrub handle	10 — More settings (quality, overlays, rotate)
4 — Previous 5 seconds	11 — Mute/Volume control
5 — Pause	12 — Zoom control
6 — Next 5 seconds	13 — Full screen
7 — Time information	14 — Thumbnail (shown on hover)

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	
1	Time Slide Bar: Changes the section of the overall timeline that is shown. The size and position of the slide bar
2	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.
3	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.
4	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.
5	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.

Media Player Actions

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

Action	Steps
Play	Click  (play icon)
Play faster or slower	Click  1X (playback speed selector) and select the speed. You can choose from half-speed (0.5X), standard speed (1X), double speed (2X), or quadruple speed (4X).
View thumbnails	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.
Jump ahead or back	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.
Skip back or forward 5 seconds	Click  (previous icon) or  (Next icon) The video jumps back or forward 5 seconds.
Pause	Click  (pause icon)
View frame by frame	While playback is paused, click  (previous frame icon) or  (next frame icon).
Zoom in or out	Click  (zoom control) and click and drag the zoom slider as needed.
Adjust contrast or brightness	Click  (filters icon) and click and drag the Contrast and Brightness sliders as needed.

Action	Steps
View full screen	To enter full screen viewing mode, click  To exit full screen viewing mode, click  .
Rotate view	1. Click  (more settings icon). 2. Click  (rotate icon).
Change video quality	1. Click  (more settings icon). 2. Click Quality and select the video quality that you want.
Mute, unmute, or control volume	To mute audio, click  (volume control icon). To unmute audio, click  (volume control icon). To raise or lower the audio volume, hover over the volume control to show the volume slider, click and drag the slider as needed.

Multicam Playback

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 3, Axon Body 2, Axon Flex 2, and Fleet system cameras 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.

[< BACK TO EVIDENCE](#)
[LAUNCH MULTICAM](#)

ADD UP TO 4 VIDEOS

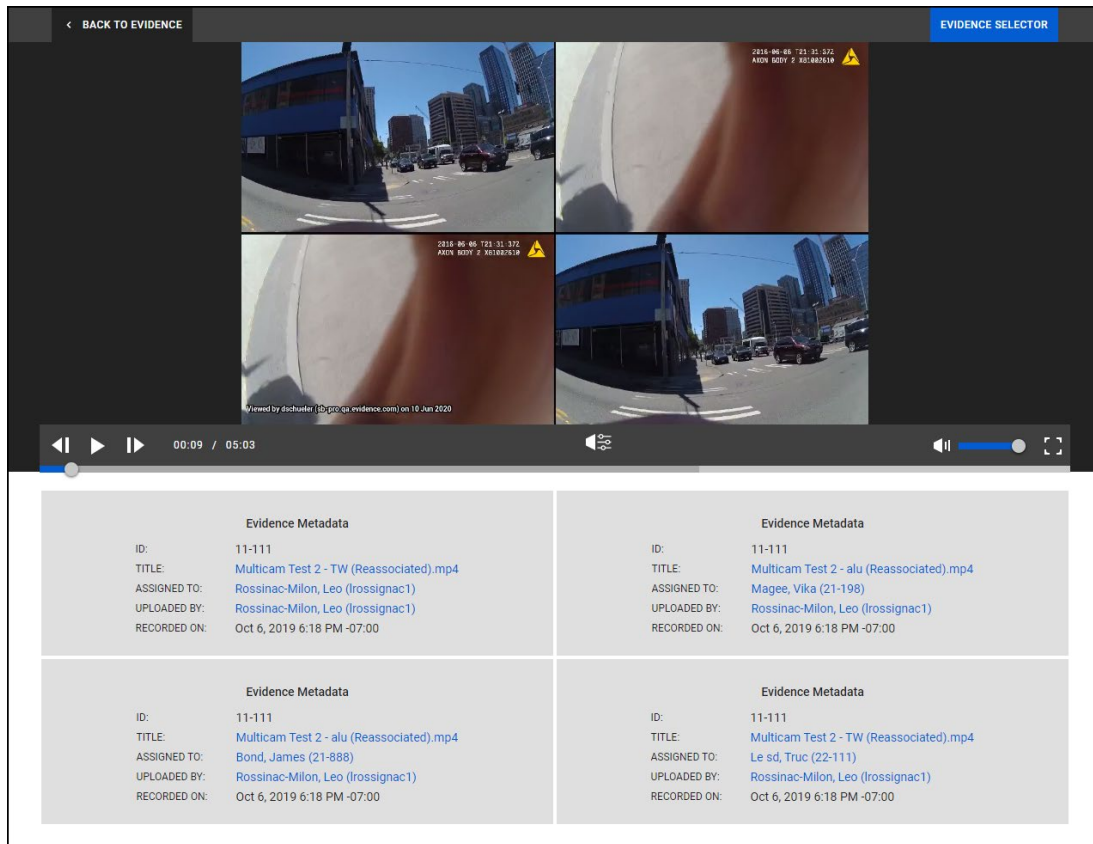
7 Items Found | 4 Selected

[UPDATE ID](#)
[DOWNLOAD](#)
[ADD TO CASE](#)

<input type="checkbox"/>	ID	TITLE	ASSIGNED TO	UPLOADED BY	UPLOADED ON	RECORDED ON
<input checked="" type="checkbox"/>	11-111	Multicam Test 2 - TW (Reassociated).mp4	Rossinac-Milon, Leo (trossignac1)	Rossinac-Milon, Leo (trossignac1)	Oct 6, 2019 6:20 PM -07:00	Oct 6, 2019 6:18 PM -07:00
<input checked="" type="checkbox"/>	2	11-111 Multicam Test 2 - alu (Reassociated).mp4	Magee, Vika (21-198)	Rossinac-Milon, Leo (trossignac1)	Oct 6, 2019 6:19 PM -07:00	Oct 6, 2019 6:18 PM -07:00
<input type="checkbox"/>	11-111	Multicam Test test - MB	Bohlender, Mike (mike1)	Bohlender, Mike (mike1)	Jun 6, 2016 3:03 PM -07:00	Jun 6, 2016 2:32 PM -07:00
<input type="checkbox"/>	None	Multicam Test 2 - alu	Lu, Alex (999)	Lu, Alex (999)	Jun 6, 2016 3:13 PM -07:00	Jun 6, 2016 2:31 PM -07:00
<input checked="" type="checkbox"/>	3	11-111 Multicam Test 2 - alu (Reassociated).mp4	Bond, James (21-888)	Rossinac-Milon, Leo (trossignac1)	Oct 6, 2019 6:19 PM -07:00	Oct 6, 2019 6:18 PM -07:00
<input type="checkbox"/>	None	Multicam Test 2 - TW	Weisz, Tamas (tw007)	Weisz, Tamas (tw007)	Jun 6, 2016 3:30 PM -07:00	Jun 6, 2016 2:31 PM -07:00
<input checked="" type="checkbox"/>	4	11-111 Multicam Test 2 - TW (Reassociated).mp4	Le sd, Truc (22-111)	Rossinac-Milon, Leo (trossignac1)	Oct 6, 2019 6:20 PM -07:00	Oct 6, 2019 6:18 PM -07:00

1. 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.
2. Optionally, you can choose **Update ID** to enter an updated ID for the selected videos, **Download** the selected videos (the videos are not combined into a single video), or **Add to Case** to add the selected videos to an existing case.
3. When all the videos have been selected, click **Launch Multicam**.
4. 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.

Action	Steps
Multicam Audio Control	<p>To select the audio track for multicam playback, click  and click on the video.</p> <p>To view which audio track is being used, hover over  and the  icon is shown.</p> <p>Audio volume is still controlled by the audio slider.</p>

Combined Multicam Video Extraction

Users can choose to extract the videos they selected for Multicam playback into a single video file. After the file is extracted, the video is treated as any other file and can be redacted, transcribed, clipped, marked, shared, or downloaded. The file can be viewed in Axon Evidence and outside of Axon Evidence as single video file.

To extract a combine Multicam video file:

1. Select which audio track will be used for the extracted file. Only one track can be used in the file. The audio track for Multicam playback is selected by clicking the audio selector icon and then clicking on the number for the appropriate video.
2. Click **Extract** to review the information, then click **Extract** again to start the process.

When the file is ready, Axon Evidence.com will send you an email to let you know the Multicam extraction is ready. The email includes a link to the new video. Clicking the link takes you to the video. This video is treated as any other file in Axon Evidence.

Requesting Human Transcriptions

Note: Your agency must have Transcription Service enabled and your User Role must have Order Transcript permission to use this functionality.

If you are looking for information on using the Axon Auto-Transcribe feature, see the [Axon Auto-Transcribe section](#) of this guide.

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.

1. When viewing evidence, select the **Transcript** tab.
2. Click **Order Transcript**.
3. Select if your evidence is in English or a mix of English and Spanish. Transcriptions with English and Spanish will cost more than English only transcriptions.

4. 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.

Transcription Order Form

LANGUAGE

☐ English (\$)
 ☐ English & Spanish (\$\$\$)

TRANSCRIPTION INSTRUCTIONS

Please input information about this evidence to help improve your transcript result. For example, number of subjects in video, names, special instructions, etc.

☐ Receive email notification when transcript is complete

CANCEL


ORDER TRANSCRIPT

5. 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.



SpeakWrite Transcript
 Ordered on 11/14/2016 11:45 AM | ORDER SUBMITTED TO SPEAKWRITE

The following table provides descriptions of the order status.

Status	Description
Order Submitted	The transcription order is being sent to the transcription service.
Order Received	The transcription order has been received by the transcription service, but has not been placed in a transcription queue.
Order Queued for Transcription	The transcription order is waiting to be processed.
Transcription in Progress	The transcription service is processing the transcription.
Order Complete	<p>The transcription is complete, added to Evidence.com, and can be viewed from the Evidence page.</p> <p>If the email notification option was selected when ordering the transcript, an email notification is sent to the user,</p>

Status	Description
Order On Hold	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.
Canceled Order	The transcription order has been canceled. Note that orders can be reopened within 45 days of cancellation.
Failed to Send	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.
Order Failed	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. You might need to contact your Evidence.com administrator to get this information.
Account Creation Error	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.
Order Reopened	The transcription service is reprocessing the transcription order.

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.

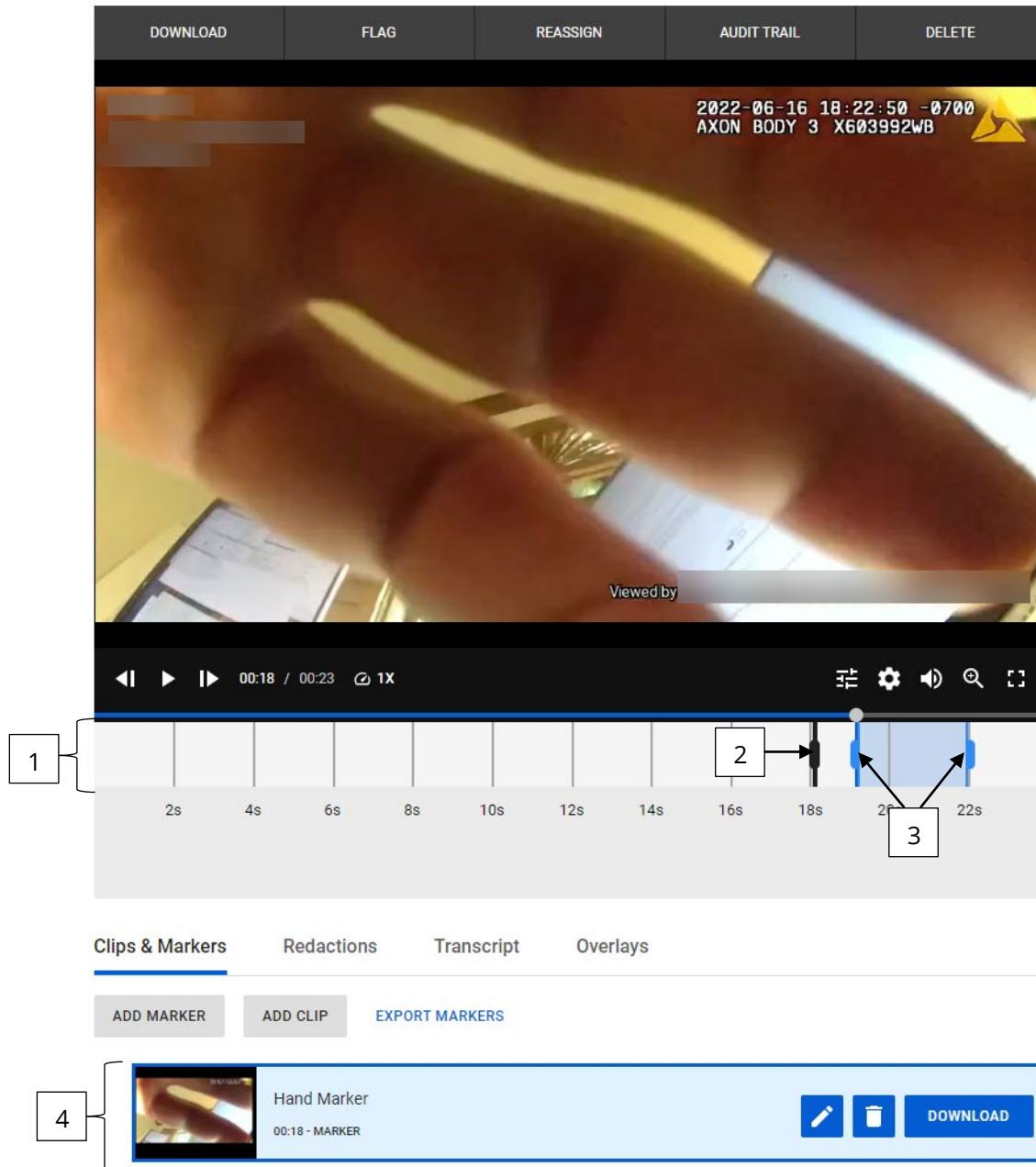
For video evidence, a marker is associated with single frame of a video evidence file. You can also download the marker as a picture file.

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.



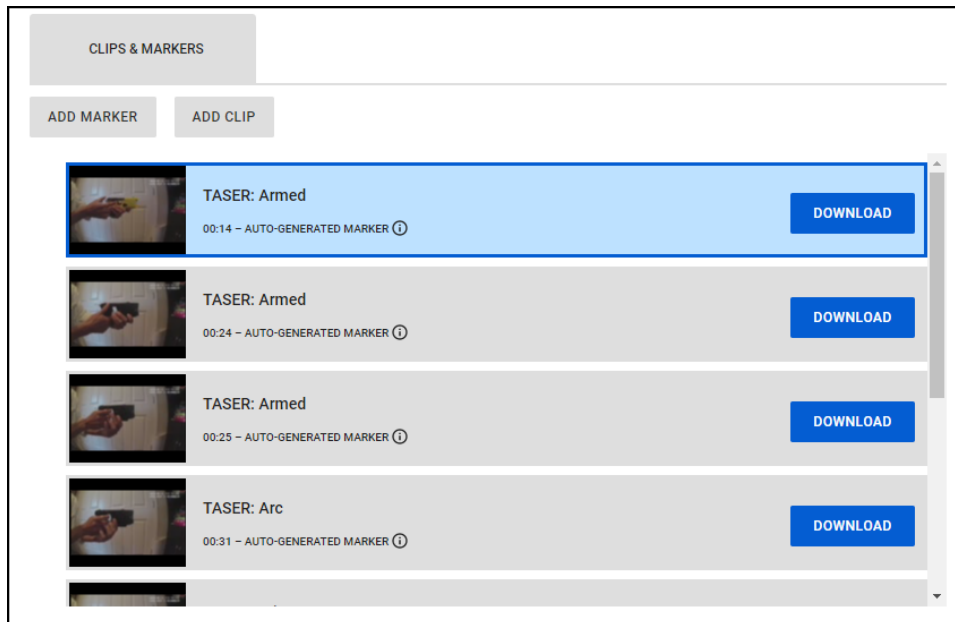
Marker and Clip Controls	
1 — Timeline	3 — Clip handles
2 — Marker handle	4 — Markers and clips list

Hypermedia Markers

When enabled for your agency, the Hypermedia Markers feature automatically adds a marker to Axon Body 3, Axon Body 2 and Axon Flex 2 camera recordings when a TASER CEW is armed, arced or deployed, or when an Axon Signal-Sidearm weapon is drawn.

Note: The Hypermedia Marker feature requires Axon Body 3 Operating System v1.11 and Axon Body 2/Flex 2 firmware v1.25.

The TASER and Signal Sidearm events are shown as markers in the video timeline and Clip and Markers section.

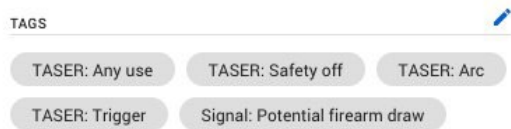


Hovering your cursor over the information icon in the marker shows information about the event, including the type and serial number of the device that initiated the marker.

'Armed' event was detected from a TASER X2 (X29002570) during the recording of this video.

Note: Only one marker is generated for an event type (arc, trigger, firearm draw) that occurs in a 40 second timeframe from a single device.

In addition to adding markers, tags for the TASER and Signal Sidearm actions are automatically added to the video. The tags cannot be removed from the video. These tags help ensure that key events are not missed during review, helping agencies manage risk and improve performance.



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 title can be a maximum of 3,000 characters in length.

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**.

The marker title can be a maximum of 3,000 characters in length.

Axon Evidence 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.

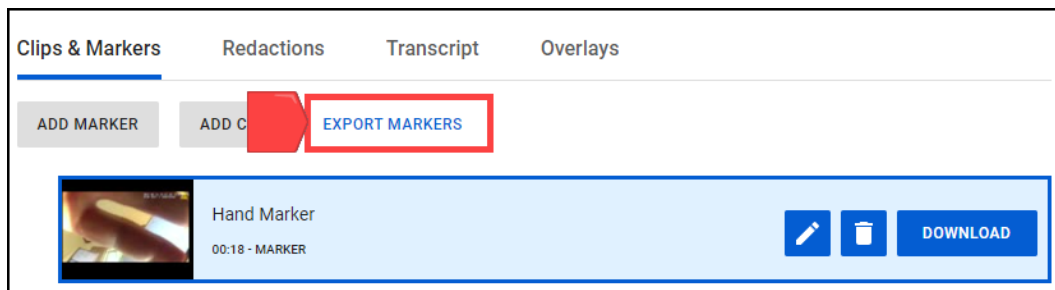
Export a Marker Report

You can export the list of evidence markers to a PDF document. The PDF shows the evidence metadata and the list of markers with the timestamps and marker description.

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. Click **Export Markers**.



The Marker Report PDF document opens in a new browser tab.

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.	<ol style="list-style-type: none"> 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.	<ol style="list-style-type: none"> 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.

Action	Steps
Move the start or end handle.	<ol style="list-style-type: none">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.	<ol style="list-style-type: none">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**.

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 (Legacy Redaction Tools)

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.

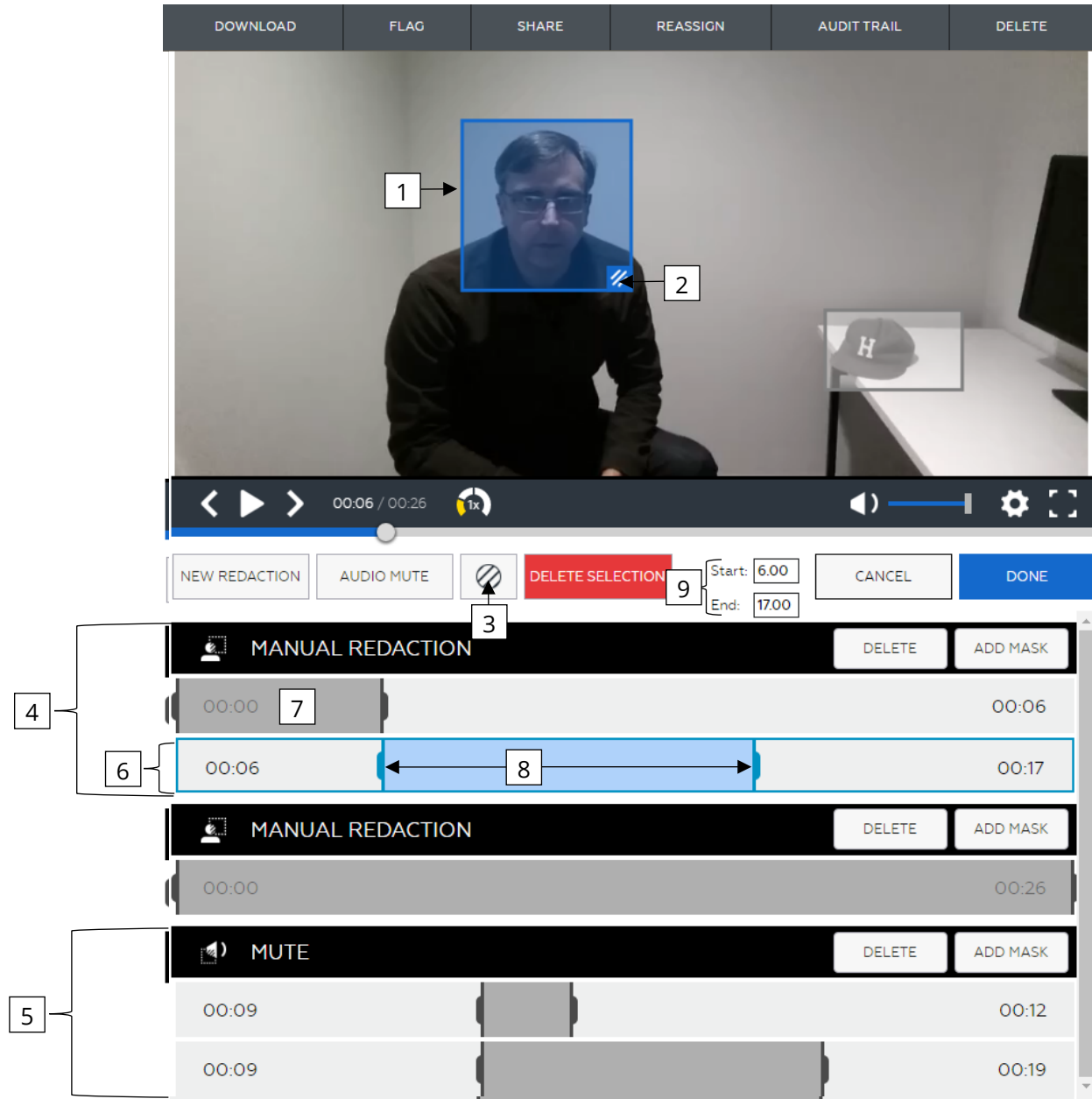
Manual redactions allow small height and width, for better redaction of small objects.

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 level of blur:

	Light blur		Heavy blur
	Medium blur		Blackout

Manual Redaction Controls



Manual Redaction Controls		
1 — Mask frame	4 — Video object	7 — Mask segment
2 — Mask frame handle	5 — Mute object	8 — Mask segment handles
3 — Blur level selector	6 — Mask timeline	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](#).

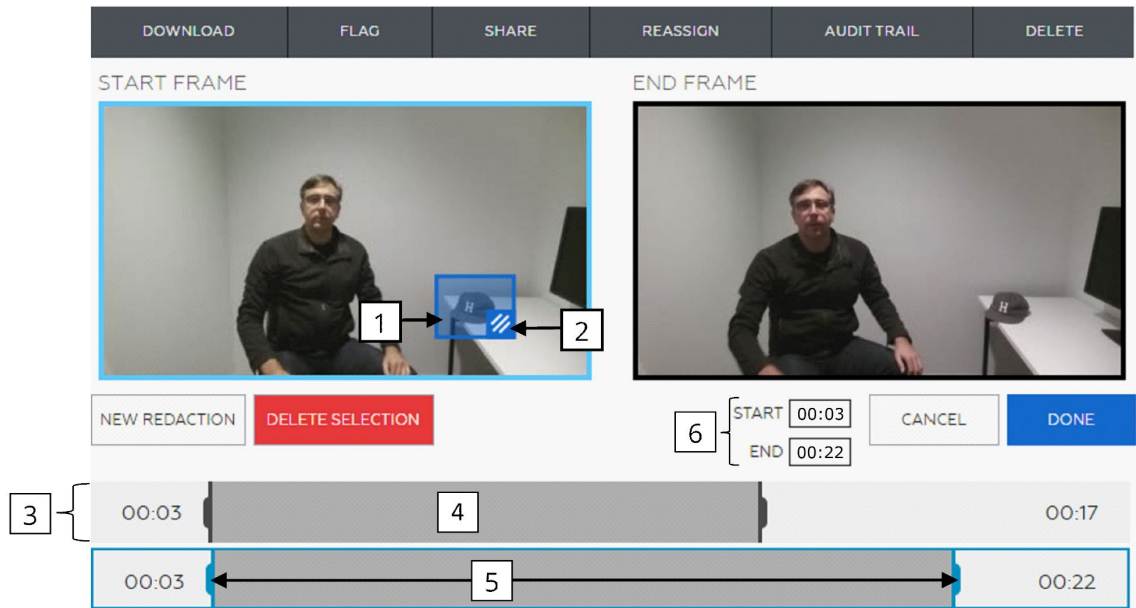
Because Smart Tracker technology automatically tracks objects in the video file, the assisted redaction feature represents an object and its timeline with one control, eliminating the need for you to create multiple mask timelines per object.

- **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.

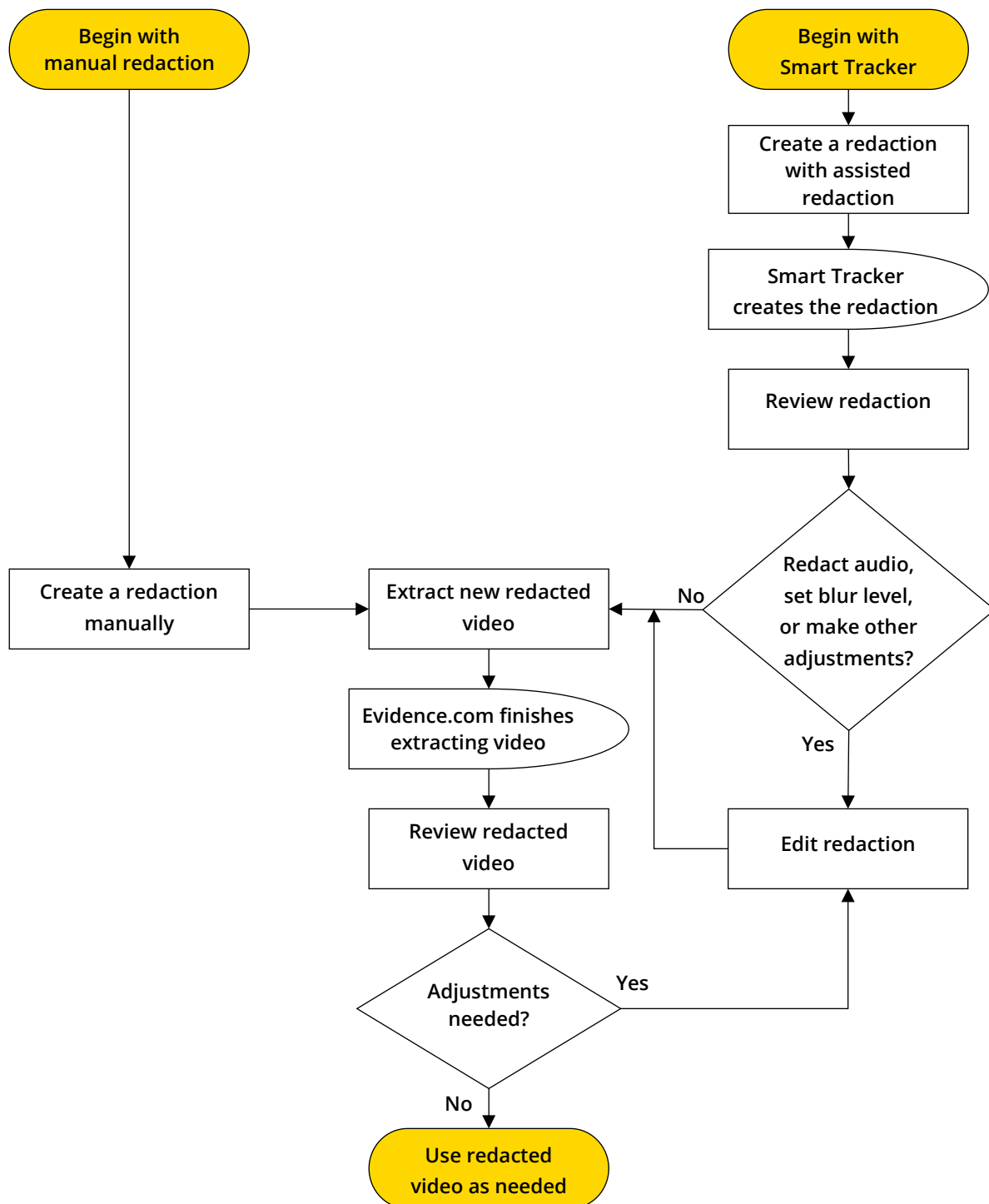
Smart Tracker Assisted Redaction Controls



Assisted Redaction Controls	
1 — Mask frame	4 — Mask segment
2 — Mask frame handle	5 — Mask segment handles
3 — Object and object timeline	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.



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.

3. Select **Manual Redaction** and click **Start**.

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.

Action	Method
Add a mask segment to an object	At the right end of the object, click Add Mask .
Delete a mask segment from an object	<ol style="list-style-type: none"> 1. If the mask segment is not blue, click the mask segment. Blue indicates that the mask segment is selected. 2. Click Delete Selection.

Action	Method
Move a start or end mask segment handle	<p>To place a mask handle approximately at the frame you need:</p> <ol style="list-style-type: none"> 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. <p>To move a mask handle one frame at a time:</p> <ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> ○ 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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 <i>mm:ss</i> format, where you want the start handle. 3. In the End box, enter the exact time in minutes and seconds, in <i>mm:ss</i> format, where you want the end handle.
Move a mask frame in a mask segment	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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.

Action	Method
Change the blur level of a mask	<ol style="list-style-type: none"> 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.

Action	Method
Add a video object	<p>Click New Redaction.</p> <p>A new object appears in the list of objects. Each new object contains one mask segment.</p>
Add the Mute object	<p>Click Audio Mute.</p> <p>The Mute object appears below the video objects.</p>
Delete an object	<p>At the right end of the object that you want to add a mask segment to, click Delete.</p> <p>The object and any mask segments it contained are removed from the redaction.</p>

4. If you need to edit mask segments or masks, use the methods provided in the following table.

Action	Method
Add a mask segment to an object	At the right end of the object, click Add Mask .
Delete mask segment from an object	<ol style="list-style-type: none"> 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	<p>To place a mask handle approximately at the frame you need:</p> <ol style="list-style-type: none"> 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. <p>To place a mask handle precisely at the frame you need:</p> <ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> ○ 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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 <i>mm:ss</i> format, where you want the start handle. 3. In the End box, enter the exact time in minutes and seconds, in <i>mm:ss</i> format, where you want the end handle.

Action	Method
Move a mask frame in a mask segment	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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.

Action	Method
Move the start or end mask segment handle	<p>To place a mask handle approximately at the frame you need:</p> <ol style="list-style-type: none"> 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. <p>To place a mask handle precisely at the frame you need:</p> <ol style="list-style-type: none"> 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: <ul style="list-style-type: none"> ○ 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.

Action	Method
Move both mask segment handles together	<ol style="list-style-type: none"> 1. On the object 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	<ol style="list-style-type: none"> 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 <i>mm:ss</i> format, where you want the start handle. 3. In the End box, enter the exact time in minutes and seconds, in <i>mm:ss</i> format, where you want the end handle.
Move the mask frame in a mask segment	<ol style="list-style-type: none"> 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 is red. 2. In the start frame, click and hold the mask frame, avoiding the handle at the lower-right corner of the frame. 3. Drag the frame to where you want it. 4. Release the mouse button.
Shape a mask frame	<ol style="list-style-type: none"> 1. Click the mask segment in order to ensure that you are shaping the correct mask frame. In the player, the mask frame 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.

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.

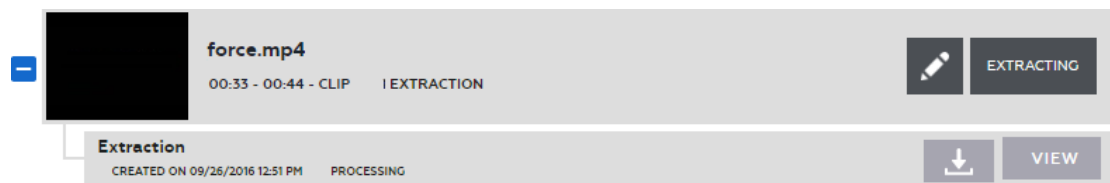
1. On the Evidence Detail page, below the video player, click **Redactions**.

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".



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.

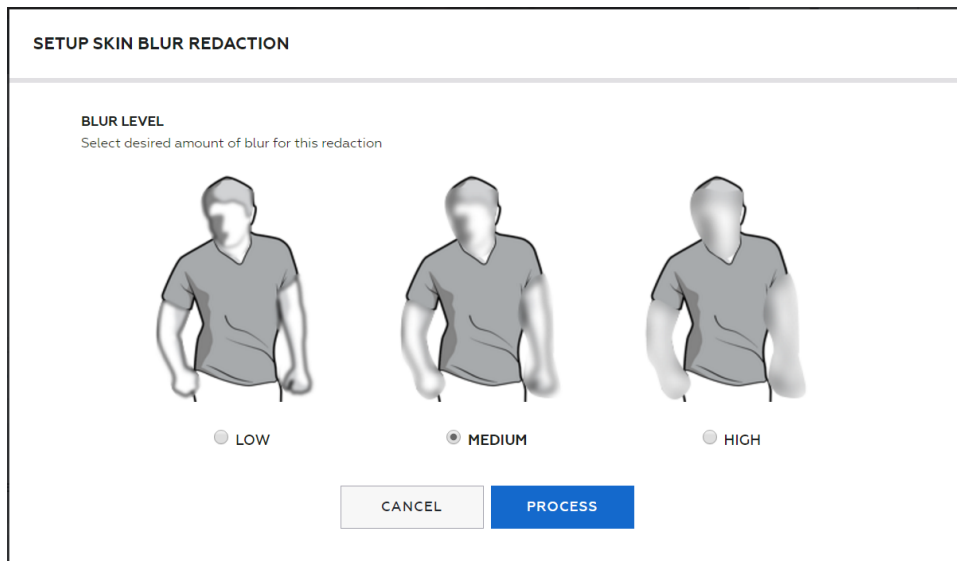
1. On the Evidence Detail page, below the video player, click **Redactions**.

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**.



SETUP SKIN BLUR REDACTION

BLUR LEVEL
Select desired amount of blur for this redaction

☐ LOW ☒ MEDIUM ☐ HIGH

CANCEL 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.

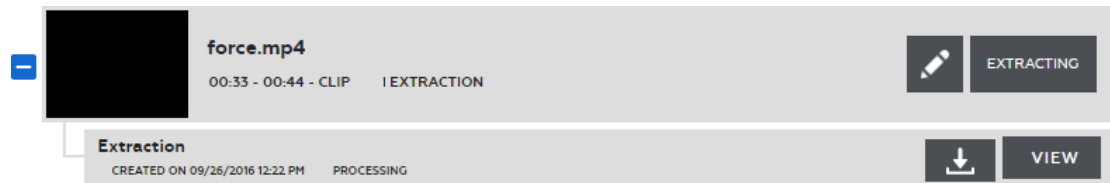
View Evidence Extracted from Clips, Markers, and Redactions

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 can 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

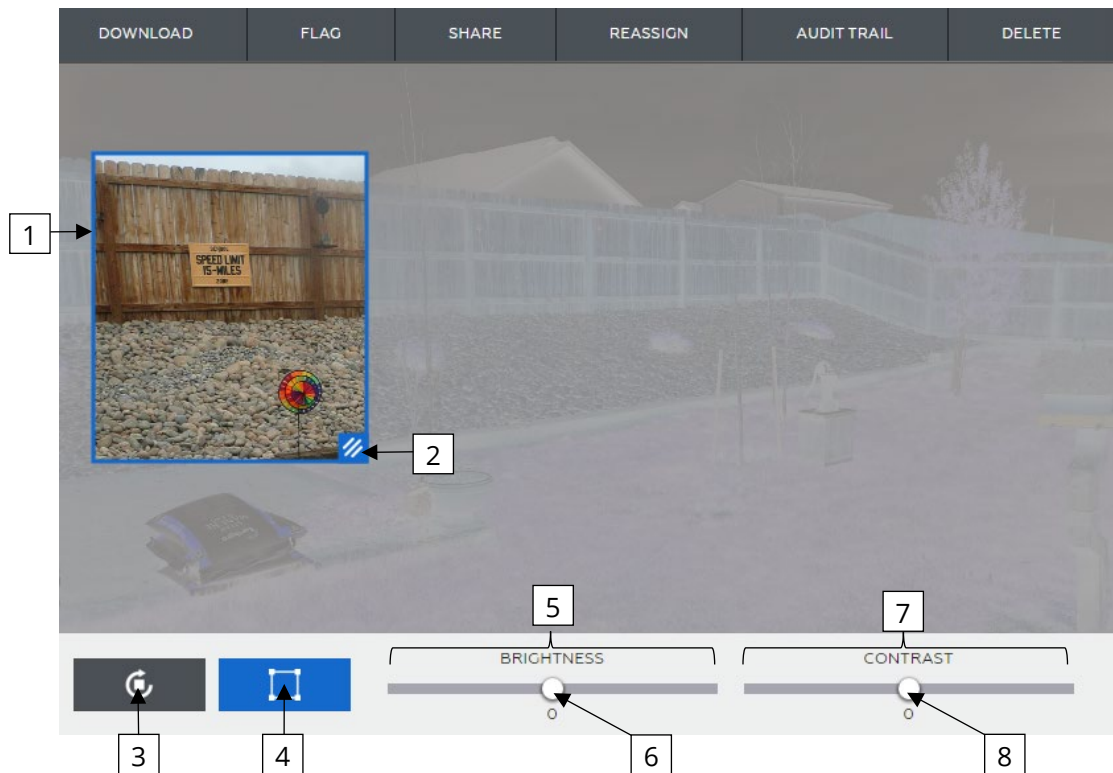
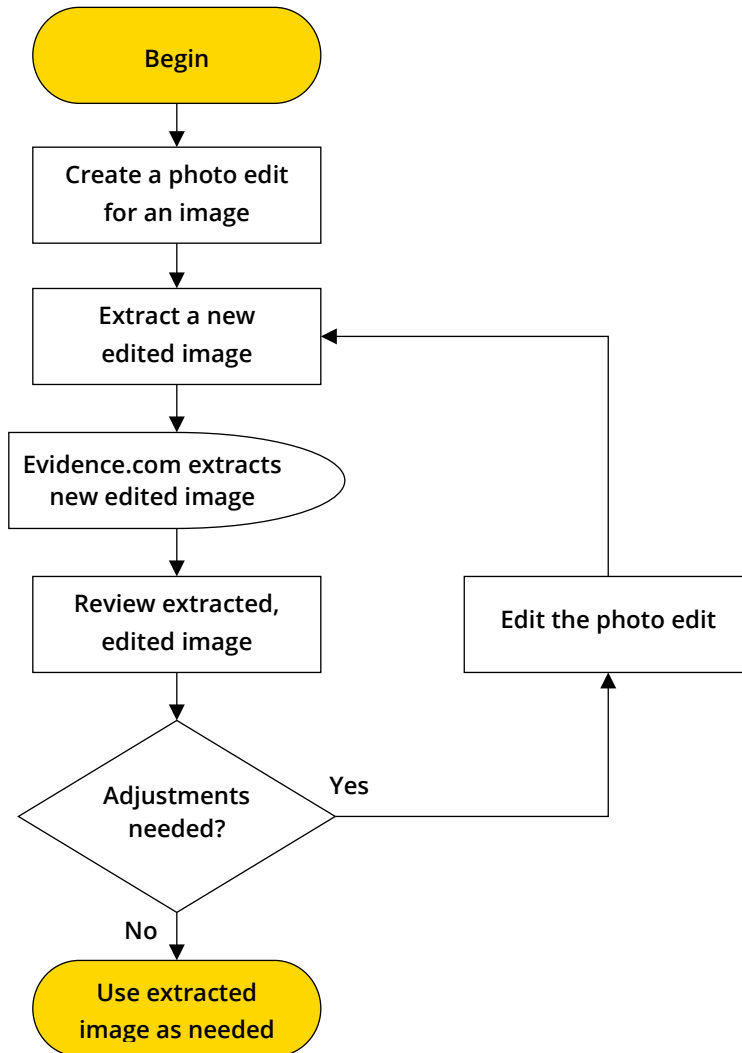


Image Tool Controls	
1 — Cropping frame	5 — Brightness slider
2 — Cropping frame handle	6 — Brightness slider handle
3 — Rotate	7 — Contrast slider
4 — Crop	8 — Contrast slider handle

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.




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.

Action	Steps
Rotate image	<ol style="list-style-type: none"> 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.
Crop image	<ol style="list-style-type: none"> 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. 2. On the image, click and hold the cropping frame, avoiding the handle at the lower-right corner of the frame. 3. Drag the frame to where you want it. 4. Release the mouse button. 5. At the lower-right corner of the frame, click and hold the cropping frame handle. 6. Drag the corner to where you want it. 7. Release the mouse button. 8. Until the frame position and shape are as needed, continue to move and shape the cropping frame.
Adjust brightness	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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. 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.

Action	Steps
Rotate image	<ol style="list-style-type: none"> 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	<p>Click .</p> <p>The cropping frame no longer appears on the image.</p>
Adjust image cropping	<p>If the cropping frame does not appear on the image, click .</p> <p>To adjust the <i>position</i> of the cropping frame:</p> <ol style="list-style-type: none"> 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. <p>To adjust the <i>shape or size</i> of the cropping frame:</p> <ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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".



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.

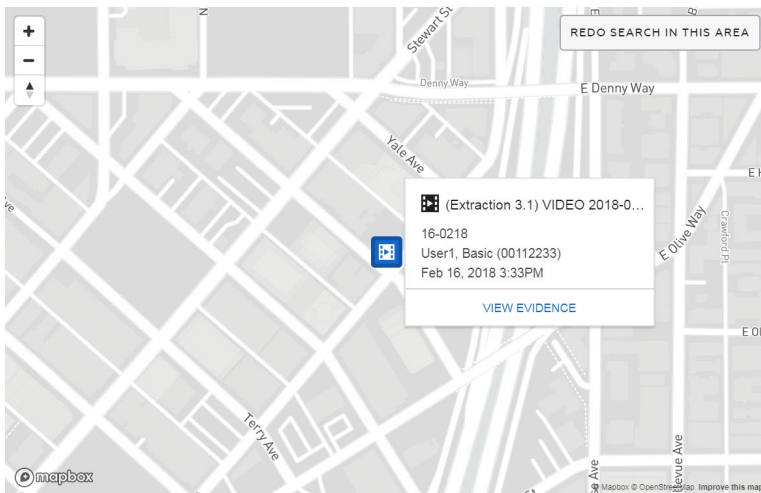
Basic Map Actions

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.

Action	Steps
Pan	<ol style="list-style-type: none"> 1. Position the mouse pointer over the map. 2. Click and hold the mouse button. 3. Move the mouse to pan the map. 4. Optionally, click Redo Search in this Area to see additional evidence in the new map view.
Zoom In or Zoom Out	<ul style="list-style-type: none"> • In the map, click on the + or – icons to zoom in or out. <p>Alternately, if your mouse has a mouse wheel:</p> <ol style="list-style-type: none"> 1. Position the mouse pointer over the map. 2. Rotate the mouse wheel to zoom in or out. <p>If needed, click Redo Search in this Area to see additional evidence in the new map view.</p>

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.

Filter	Steps
Location	<ol style="list-style-type: none"> 1. Click in the Location field. 2. Type in an address, city, or zip code. 3. Optionally, select
User	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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.

Publish to Social Media

The Publish to Social Media feature allows authorized users to share video directly from the Evidence Detail page in Axon Evidence to social media websites. The Publish to Social Media feature currently supports publishing to YouTube and we expect to add additional social media platforms in future releases.

If your agency is interested in having the Publish to Social Media feature at your agency, contact your Axon representative.

See [Social Media Publishing](#) for information on enabling the Publish to Social Media feature once it is activated for your agency.

Publish to Social Media Permission

Users must have the **Publish to Social Media** permission enabled for their Role to publish content directly to approved social media platforms. The Publish to Social Media permission requires that the Unrestricted Evidence View permission is not set to Prohibited.

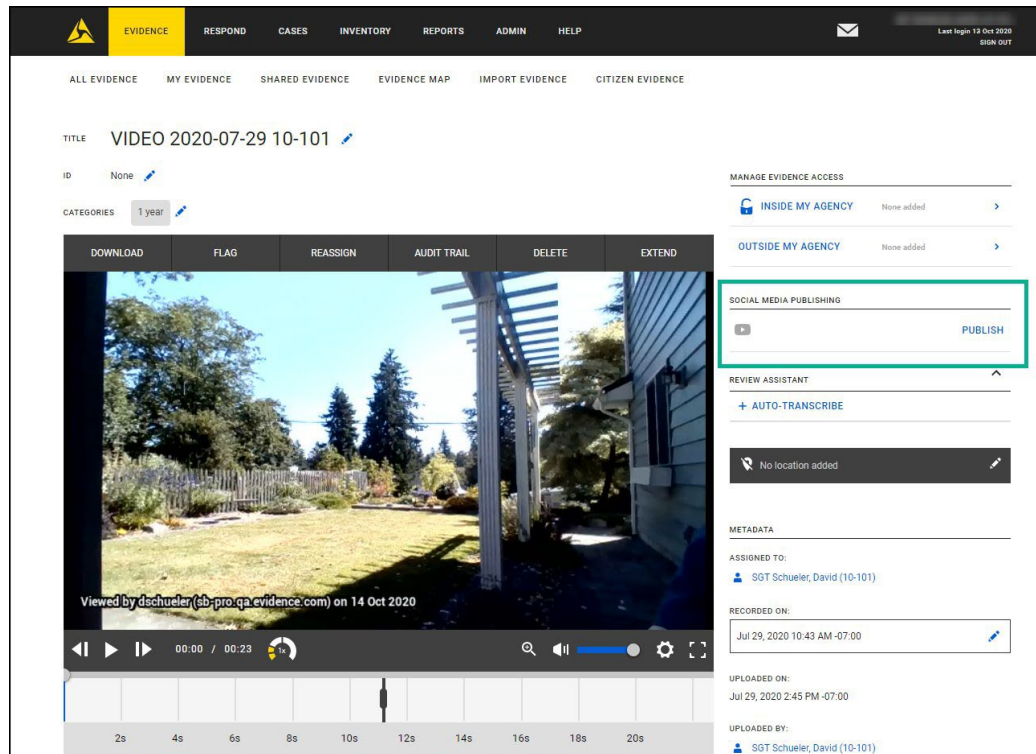
Agency Axon Evidence administrators should modify or create new Roles and enable the Publish to Social Media permission for the Roles.

Share	<input checked="" type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Publish to Social Media	<input checked="" type="radio"/> Allowed	<input type="radio"/> Prohibited		
Restrict	<input checked="" type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited

Publishing to Social Media

Users with the Publish to Social Media permission can share videos to social media websites from the Evidence Detail Page.

1. From the Evidence Detail page in the Social Media Publishing section, click **Publish**.



The Publish to Social Media screen is shown on the right side of the page.

2. Select the Social Media Platforms where you want to publish the video.

Note: you may need to connect to your agency's social media account before publishing.

3. Enter the Title, Description, and Tags as needed
4. Click **Publish**. The system asks the user to confirm the social media platforms where the video will be published.

When the video is published, the date the video was published and the user that published it is shown on the Evidence Detail Page. The evidence audit trail includes detail about this publication and a link to the external platform page where the video was made available.

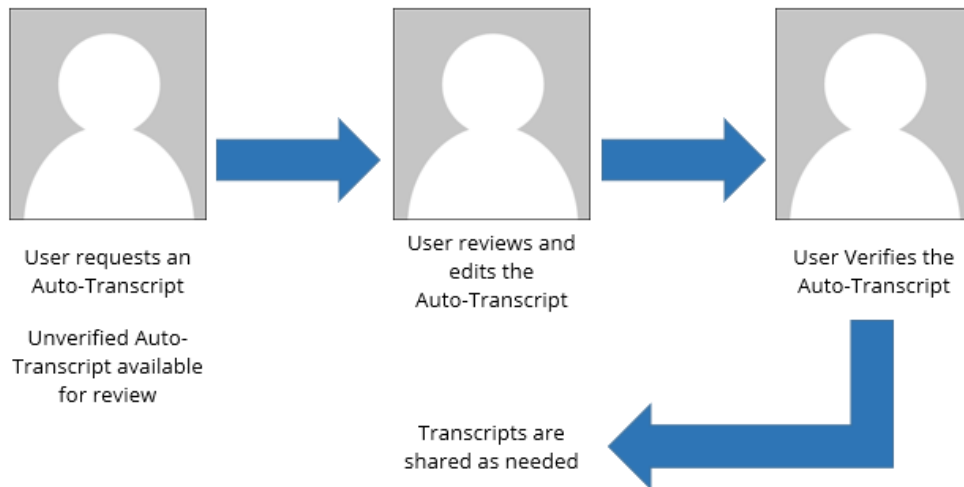
Axon Auto-Transcribe

Video and audio evidence are central to every investigation. But the sheer quantity of this evidence increases the time officers and prosecutors must spend reviewing it - plus it can be mentally draining to listen to disturbing audio or see graphic images over and over again.

Axon Auto-Transcribe with Fast Evidence Review and Transcription Assistant allows your agency to transform the way you review and transcribe evidence. No more having to watch every minute of a piece of digital evidence. Simply scan the auto-transcript to quickly survey what happened or search for key words. When it comes time for 100% accuracy, you can quickly produce a court-ready transcript in a fraction of the time and cost required by human transcription.

Axon Auto-Transcribe uses the power of artificial intelligence (AI) to accelerate the review and transcription of evidence, creating significant time and cost saving benefits for agencies. Instead of viewing video, audio, and text as separate elements from an incident, Axon Auto-Transcribe unifies all these elements into one “hypermedia player” enabling powerful connections and efficiencies for public safety agencies. No more having to watch every moment of digital evidence. Instead, users can simply scan the auto-transcript to quickly survey what happened and jump to the significant section by clicking on the spoken words. When it comes time to produce court-ready transcripts, Axon Auto-Transcribe can help produce the transcript in a fraction of the time and at a fraction of the cost of human transcription alone.

Auto-Transcribe Workflows



1. User with Auto-Transcribe permission opens evidence and requests an Auto-Transcript (the agency must have Auto-Transcribe minutes available).

Other users can use Fast Evidence Review to review evidence.

2. Authorized users can use Transcription Assistant to review, edit, and save changes to the Auto-Transcript.
3. Authorized users can verify the transcript changes.
4. Transcripts can be shared through evidence and case shares.

Auto-Transcribe Accuracy

We chose the best available speech recognition solution for public safety data, not only for accuracy but also for equitable performance among diverse populations. We use the highest industry standard for measuring accuracy — every letter of the word must be correct for us to get credit. On public safety data, we average 80% accuracy, reaching levels in the high 90% range as the audio gets clearer. Microphone quality and recording environment are the two biggest factors in auto-transcript accuracy. Our testing includes variations of English, encompassing several different local accents and assorted styles of body camera and interview room video. Transcription Assistant makes it incredibly easy for authorized users to make corrections.

Auto-Transcribe Licensing

Auto-Transcribe plans are implemented in one of two methods:

- **Unlimited Auto-Transcribe:** Agencies have unlimited access to Auto-Transcribe, for evidence they intend to consume. Additionally, all agency Axon body-worn camera recordings are automatically auto-transcribed. Auto-transcripts can be requested for other recordings. The agency is charged a flat per-user-per-month fee.
- **By Minutes usage:** Minutes are purchased and pooled together at the agency. The number of minutes remaining are shown when a transcript is ordered.

Note: The System Usage dashboard shows the available and used Auto-Transcribe minutes for your agency. Users assigned to a Role that has the View Unrestricted Evidence permission set to Any can view the System Usage dashboard.

As an introduction to Axon Auto-Transcribe, we have created Auto-Transcribe Starter Packs. Customers with Axon Pro licenses will receive 100 minutes per license and customers with Axon Records licenses will receive 200 minutes for each license. Customers on Axon's Officer Safety Plan 7+, which encompasses both Axon Pro and Axon Records offerings, will receive a starter pack of 300 minutes per license. These minutes are pooled within your agency and expire at the end of each calendar year.

Auto-Transcribe Permissions

Agency Axon Evidence.com administrators must enable the appropriate permissions for the Roles that will use Auto-Transcribe.

Auto-Transcribe permissions are in the Evidence Management permissions section and require a Pro license. The Auto-Transcribe permission settings and requirements are described below.

Evidence Management				
View Unrestricted Evidence	<input checked="" type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
View CEW Firing Logs	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input checked="" type="radio"/> Prohibited
Edit	<input checked="" type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Add/Remove Pending Review Category	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input checked="" type="radio"/> Prohibited
Edit Evidence Group	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input checked="" type="radio"/> Prohibited
Redact PRO	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input checked="" type="radio"/> Prohibited
Order Human Transcript PRO			<input type="radio"/> Allowed	<input checked="" type="radio"/> Prohibited
Auto-Transcribe PRO	<input type="radio"/> Any Evidence	<input checked="" type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Edit Auto-Transcript PRO	<input type="radio"/> Any Evidence	<input checked="" type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Verify & Unverify Transcript PRO	<input type="radio"/> Any Evidence	<input checked="" type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input type="radio"/> Prohibited
Reassign	<input type="radio"/> Any Evidence	<input type="radio"/> Their Groups' & Their Own	<input type="radio"/> Only Their Own	<input checked="" type="radio"/> Prohibited

- **Auto-Transcribe:** Allows the user to request an auto-transcript. This can be set to allow the user to request an auto-transcript for any evidence or only evidence belonging to the user or the user's groups. This permission requires the View Unrestricted Evidence permission.
- **Edit Auto-Transcript:** Allows the user to access and use the Transcription Assistant to edit an auto-transcript. This can be set to allow the user to edit the auto-transcript for any evidence or only evidence belonging to the user or the user's groups. This permission requires the View Unrestricted Evidence and Edit permissions.
- **Verify & Unverify Transcript:** Allows the user to verify and unverify an auto-transcript. This can be set to allow the user to verify and unverify the auto-transcript for any evidence or only evidence belonging to the user or the user's groups. This permission requires the View Unrestricted Evidence, Edit, and Edit Auto-Transcript permissions.

Fast Evidence Review

The Auto-Transcribe Fast Evidence Review is shown on the Evidence Detail page on the right-side of the evidence preview. Fast Evidence Review is used to request an auto-transcript and review the information in a transcript.

Note: Users that have permission to view the evidence, but do not have the Auto-Transcribe permission enabled for their assigned Role will only see Fast Evidence Review if a transcript has been created. Users assigned to a Pro Role that do not have Edit Auto-Transcript permission can open Transcript Assistant to review and download transcripts. Users assigned to a Basic Role can download transcripts from the Transcript tab on the Evidence Detail page.

The screenshot displays the Axon Evidence Fast Evidence Review interface. The top navigation bar includes tabs for EVIDENCE, RESPOND, CASES, INVENTORY, REPORTS, ADMIN, and HELP. The main content area shows the evidence title 'AB3_1234_9876' and its parent file 'Interview Room 1 2018-03-12 0844 - Investigation'. The categories are 'Criminal Investigation' and 'Assault'. The video player shows a timestamp of 13:25:24 05-27-10. The right sidebar contains the 'FAST EVIDENCE REVIEW' panel, which includes a search bar with 'Miranda', a 'TRANSCRIPTION ASSISTANT' button, and a transcript of a conversation. The transcript text is as follows:

Speaker 1 6:17 PM / 00:27
Wait so let me finish. You're correct, that's what I saw. I saw... I saw them get into the white van, down on Main St. It was very suspicious, especially considering that they were all dressed in the same outfits and had gloves on and whatnot. I just sort of stood there and watched this shake out.

Speaker 2 6:17 PM / 00:39
And you're sure they were the guys? They had the attire we discussed before and everything?

Speaker 1 6:17 PM / 00:48
Um, I mean. Yeah. That's what I saw. I the guys had the gloves and whatnot.

Speaker 1 6:17 PM / 00:55
Um, so therefore there's no need to fill it out for them to know. I'm going to prove they the police department **Miranda** warning she um, and buy you your rights, right.

Speaker 2 6:18 PM / 01:09
Okay so let's see here. You want me to prove that to you? Hmm, I don't know if I'm going to be able... okay fine...uh...nevermind.

Requesting an Auto-Transcript

Note: Users must have Auto-Transcribe permission enabled for their assigned Role to request a transcript.

1. Open the Evidence Detail page for the appropriate evidence.

2. Under Fast Evidence Review, click **Auto-Transcribe**.

Note: Transcript processing is recorded in the Evidence and User Audit Trails.

The screenshot shows the Axon Evidence web application interface. The top navigation bar includes 'EVIDENCE', 'RECORDS', 'AWARE', 'CASES', 'INVENTORY', 'REPORTS', 'ADMIN', and 'HELP'. The user is logged in as 'Taylor, Chester' on '06 Aug 2020'. The main content area displays details for a video titled '[Breakout] Shay Lee.mp4'. The video player shows a car's interior view. To the right, the 'FAST EVIDENCE REVIEW' section is expanded, showing a '+ AUTO-TRANSCRIBE' button highlighted with a green box. Other details include 'ASSIGNED TO: Taylor, Chester (67-891)', 'RECORDED ON: Aug 6, 2020 8:49 AM -07:00', 'UPLOADED ON: Aug 6, 2020 8:53 AM -07:00', 'UPLOADED BY: Taylor, Chester (67-891)', 'DELETION SCHEDULED FOR: Unscheduled', 'FILE FORMAT: video/mp4', and 'FILE SIZE: 167.4 MB'.

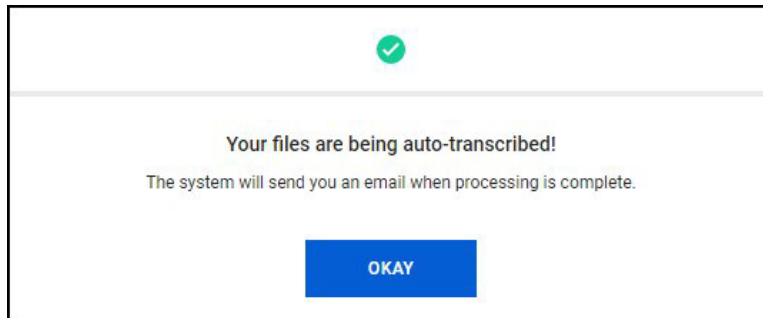
3. You are asked to confirm the request. Click **Start** to continue.

All transcript processing is done in the system background and does not impact Axon Evidence performance.

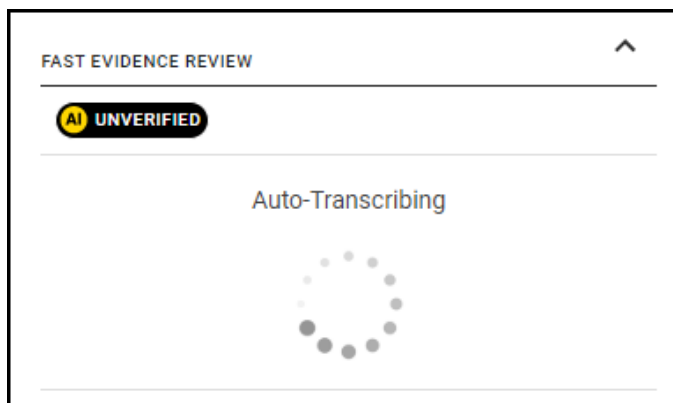
The screenshot shows a confirmation dialog box titled 'Auto-Transcribe'. It features an 'AI' icon and the text 'Auto-Transcribe Ready in 5 mins'. Below this, it says 'Press start to begin auto-transcribing your evidence. You will be able to view the auto-transcript once processing is complete.' A green checkmark icon is followed by the text '2 minutes will be used for this file and 1,000 minutes are available.' At the bottom, there are two buttons: 'CANCEL' and 'START'.

Note: For agencies on the By Minute Plan, the number of transcription minutes available is shown when confirming the request. If your agency does not have enough minutes available to complete the request, then you will not be able to complete the request.

The system confirms the request. Click **Okay** to continue.

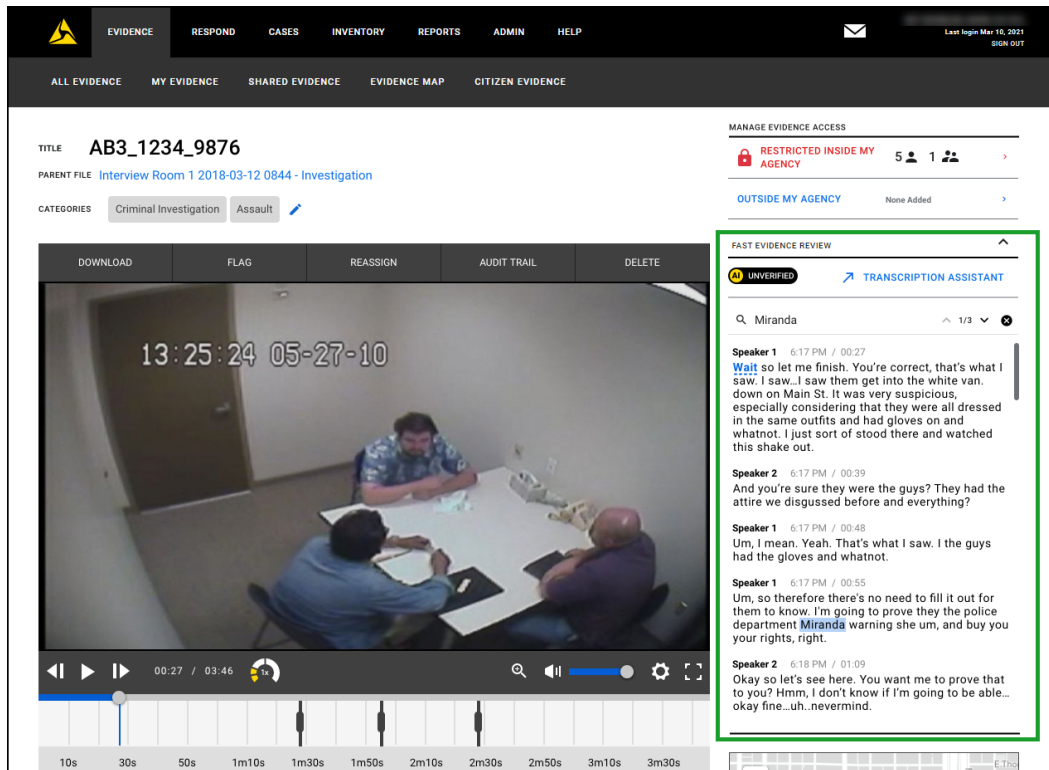


Fast Evidence Review shows the transcription is in progress. Axon Evidence will send you an email notification when the transcription is complete.



Using Fast Evidence Review

When an auto-transcript is complete, Fast Evidence Review can be used to review the information in a transcript.



- **Fast Evidence Review Navigation**

Auto-transcripts are time-synced with the video or audio file. As you play a file, the highlighted word in the transcript aligns to the current point in playback.

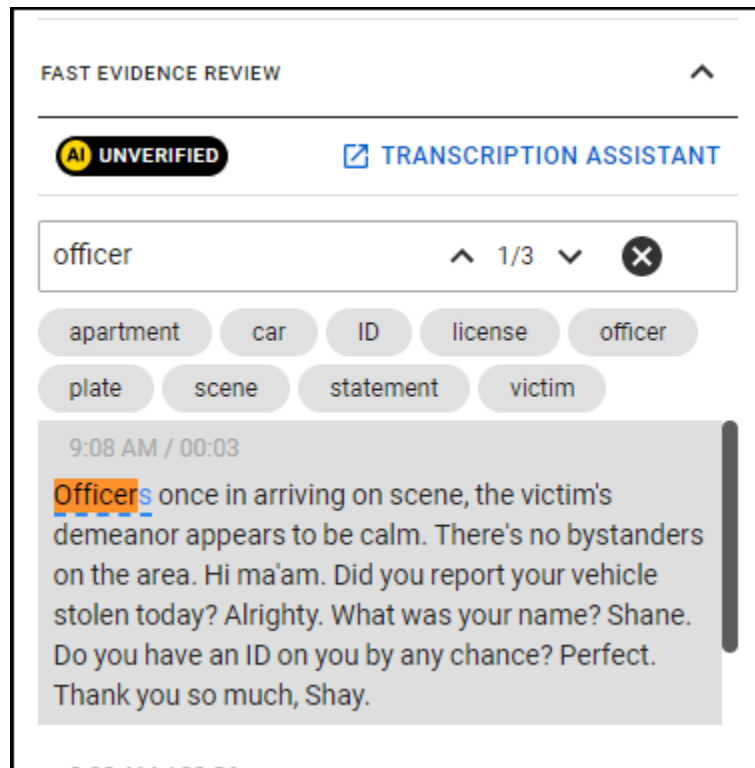
To navigate to a specific point in the file, click on the word or timestamp in the transcript.

- **Text Search**

In Fast Evidence Review the search field is above the transcript text. The system searches for exact matches after each character is entered in the search field. Matches are highlighted in the transcript. If there is more than one match, the number of matches is shown and there are arrows that let the user navigate to each match. If there is no match, number of matches show 0/0 and the arrows are inactive.

- **Discovered Keywords**

During processing the system searches the auto-transcript for common keywords and shows those words to the above the auto-transcript. Users can click the word while searching to find all instances of the common keyword. This allows users to quickly find commonly used words in the transcript and jump to the occurrences of those words in the transcript and evidence.



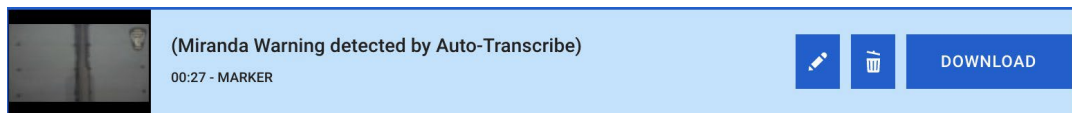
The common keywords list includes the following:

Address	Apartment	Arrest	Axon
Car	Cellphone	Channel	Charge
Child	CID	Citation	City
Complainant	Consent	County	Court
Crime	Custody	Date of birth	Deputy
Description	Detain	Direction	Driver
Drug	EMS	Evidence	Felony
Firearm	FSU	Gun	Handcuff
Handgun	Highway	Hold	Hurt
ID	Identification	Knife	License
Location	Marijuana	Miranda	Narrative
NCIC	Occupant	Officer	Pain

Passenger	Patrol	Phone	Pistol
Plate	Pursuit	Resist	Restrain
Rifle	Scene	Search	SFST
Shot	Shotgun	Sobriety	Speed
Statement	Stop	Summon	Suspect
Tag	Taser	Test	Traffic
Transport	Travel	Trooper	Truck
Victim	Warrant	Weapon	

Miranda Warning Detector

The Miranda Warning Detector automatically creates a marker in the recording when the system detects that a Miranda warning is spoken. The detection happens automatically while a file is auto-transcribed. The image below shows an example of the marker on the Evidence Detail page.



Important: The ability to detect a Miranda warning is directly correlated to the quality of the associated auto-transcript and is not 100% accurate.

The Miranda Warning Detector is enabled for all Auto-Transcribe customers in the United States.

Auto-Transcribe Bulk Requests

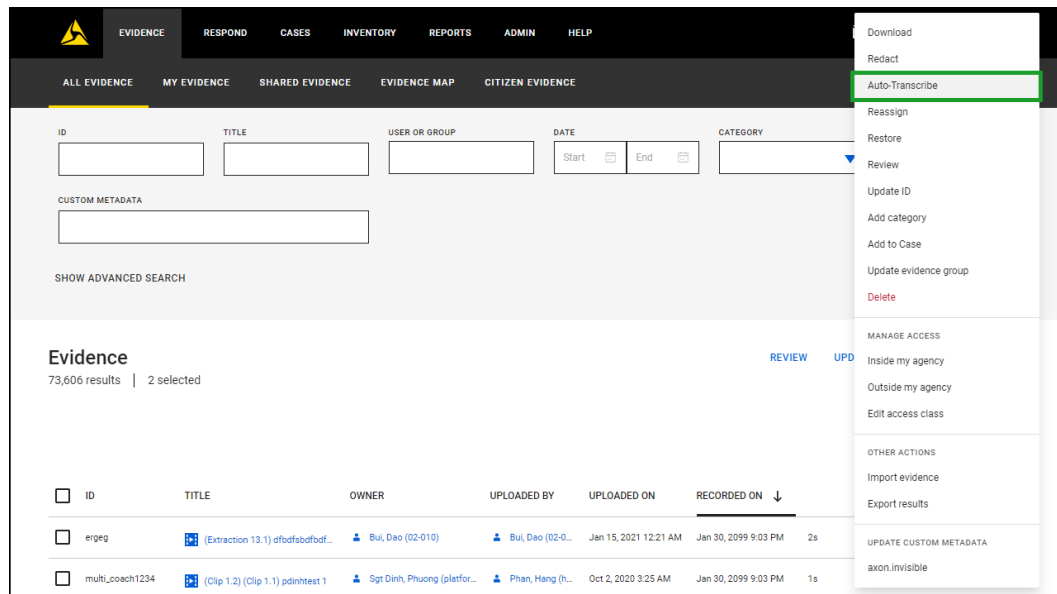
Auto-Transcribe users can request transcripts for multiple files from the Evidence Search and Case Details - Evidence tab.

Note: Axon Evidence does not send email completion notifications for files included in a bulk Auto-Transcribe request.

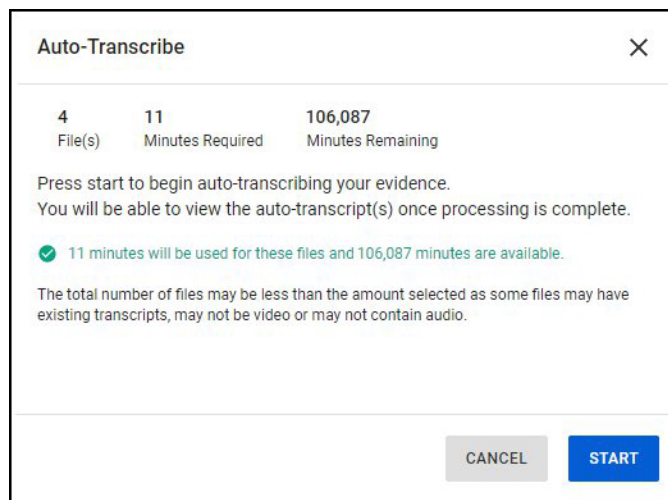
Bulk Requests from the Evidence Search Page

1. On the Evidence Search page, search for and select the video and audio files you want auto-transcribed.

- Click the ... (more actions) menu and select **Auto-Transcribe**.



The Auto-Transcribe screen is shown on the right side of the page. This screen shows the number of files selected, an estimate of the number of minutes required, and the number of minutes remaining at your agency.



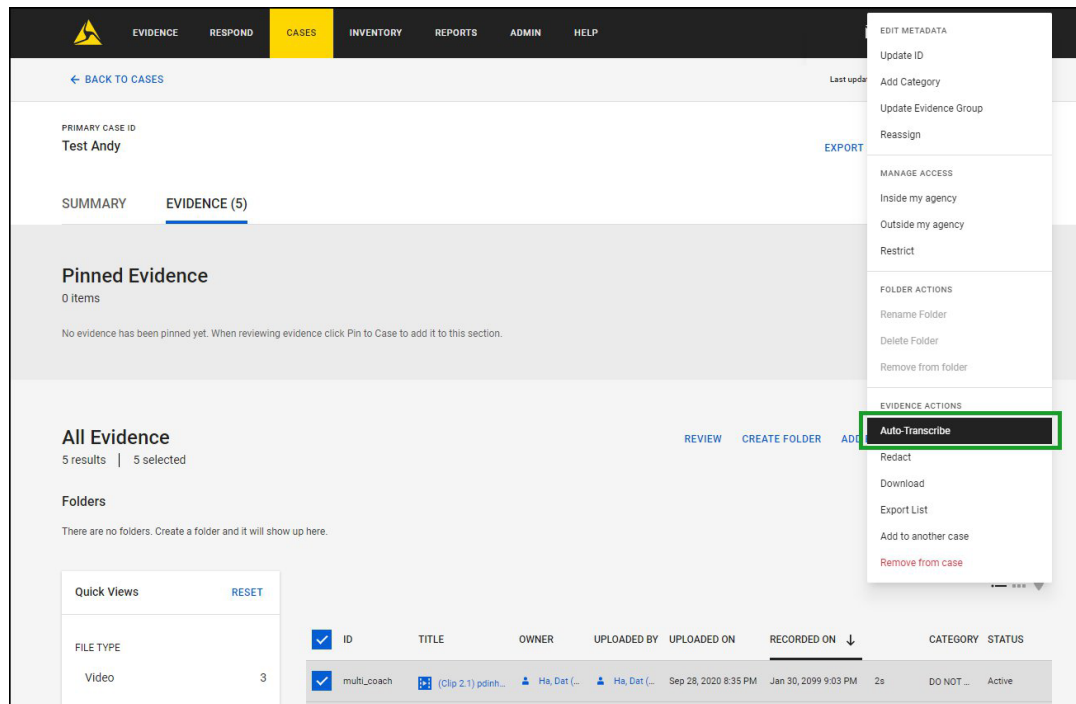
- Click **Start** to submit the request.

Once the requests are submitted, the Evidence Detail page for the selected files will show that the transcription is in process.

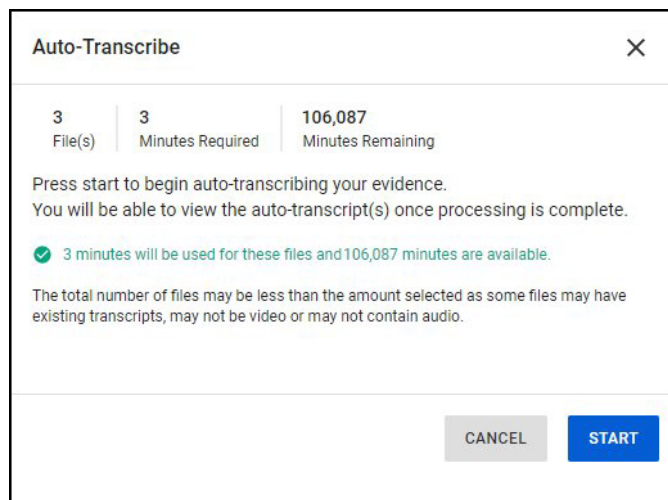
Bulk Requests from the Case Details Evidence Tab

- From the Case Details Evidence tab, find and select the video and audio files you want auto-transcribed.

- Click the secondary actions button (...) and select **Auto-Transcribe** under the Evidence Actions.



The Auto-Transcribe screen is shown on the right side of the page. This screen shows the number of files selected, an estimate of the number of minutes required, and the number of minutes remaining at your agency.



- Click **Start** to submit the request.

Once the requests are submitted, the Evidence Detail page for the selected files will show that the transcription is in process.

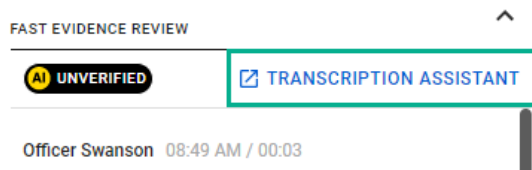
Transcription Assistant

The Auto-Transcribe Transcription Assistant is used to download, edit, and verify the content of an auto-transcript. Transcription Assistant was specifically designed to help you edit auto-transcripts as fast as possible, whether you're a full-time transcriber or only transcribing occasionally.

Note: Only unverified transcripts can be edited.

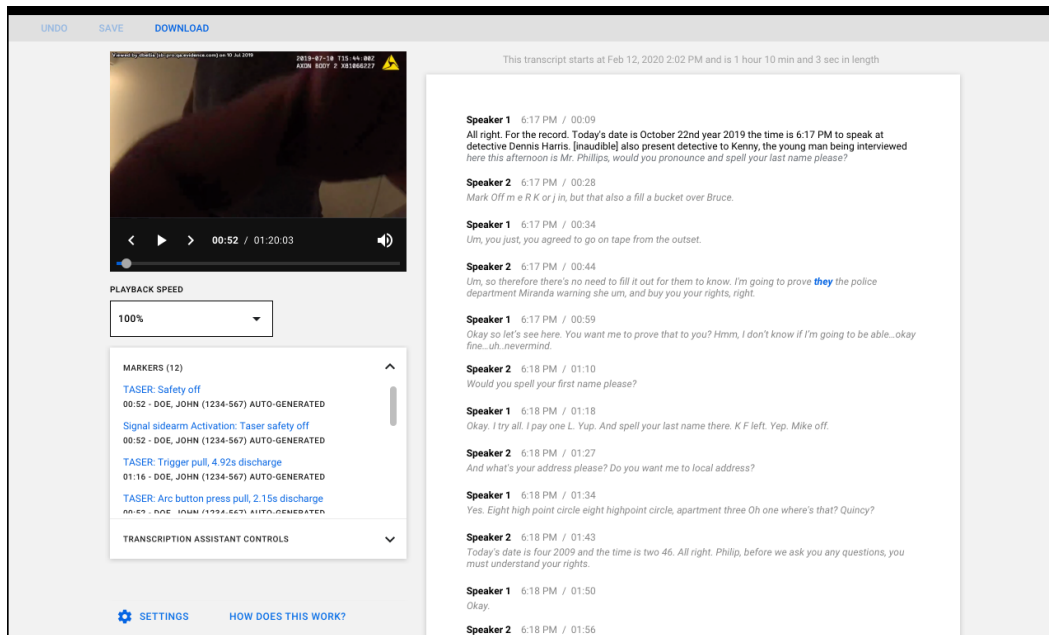
Users assigned to a Pro Role that do not have Edit Auto-Transcript permission can open Transcript Assistant to review and download transcripts. Users assigned to a Basic Role can open Transcript Assistant to download transcripts.

To open Transaction Assistant, click **Transcription Assistant** in Fast Evidence Review section of the Evidence Detail page.



To close Transcription Assistant and return to the Evidence Detail page, click the **X** in the upper right of the Transcription Assistant.

Transcription Assistant Editing Actions



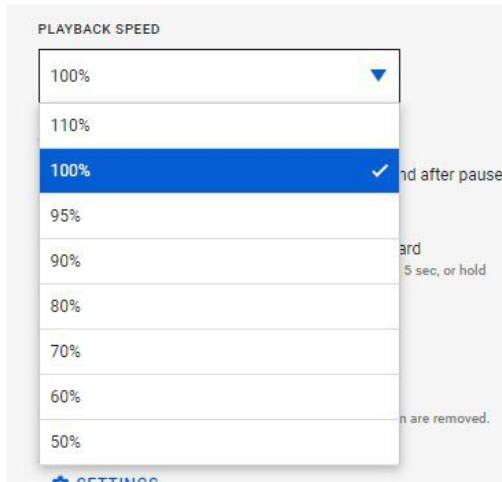
Similar to Fast Evidence Review, the auto-transcripts in Transcription Assistant are time-synced with the video or audio file, even after you have made edits. While playing the file, the word that aligns to the current point in playback is highlighted and you can navigate to a specific point in the media, click on the timestamp or single-click on any word within the Transcription Assistant text (**Note:** Jumping to the selected point in the transcript and media can be set to use a double-click in the [Transcription Assistant Settings](#)).

Transcription Assistant uses media player controls and keyboard controls for file playback. Additionally, Transcription Assistant can support foot pedal use while editing. See [Foot Pedal Support](#) for more information.

The following information outlines how to use Transcription Assistant to work with text and speaker labels.

Setting Playback Speed

The playback speed sets how fast the file is played back. Playback speed can be set from 50% - 110% of normal speed using the **Playback Speed** list under the media player.



Using Markers

The Markers list to show all the markers associated with the recording. Click the list to expand it and show all the markers. Then click a marker to jump to that point in the transcript and recording.

Working with Text

The initial auto-transcript is machine-generated and can require some human input to ensure it is accurate. You can use Transcription Assistant to edit and confirm the machine-generated text.

- **Text Search**

Fast Evidence Review leverages your browser's text search capability to search the transcript. Simultaneously press the **Ctrl + F** keys (Windows) or **Command + F** (Mac) to show the browser text search field. Type the text you want to find into the field and use the browser controls to move between instances of the text on the page.

- **Confirming Text**

Text can be confirmed during the playback or while playback is paused. When the underlined word or punctuation is correct, press the **Tab** key to confirm.

Unconfirmed text or punctuation is formatted as italic. When the text or punctuation has been confirmed, the text is shown with regular formatting. This helps you identify which parts of the text have and have not been confirmed.

Tip: To confirm long strings of words, press and hold the **Tab** key. This confirms text and punctuation to the farthest word in the transcript.

- **Editing text and handling incorrect suggestions**

When text in the auto-transcript are incorrect, type the correct word or words into Transcription Assistant.

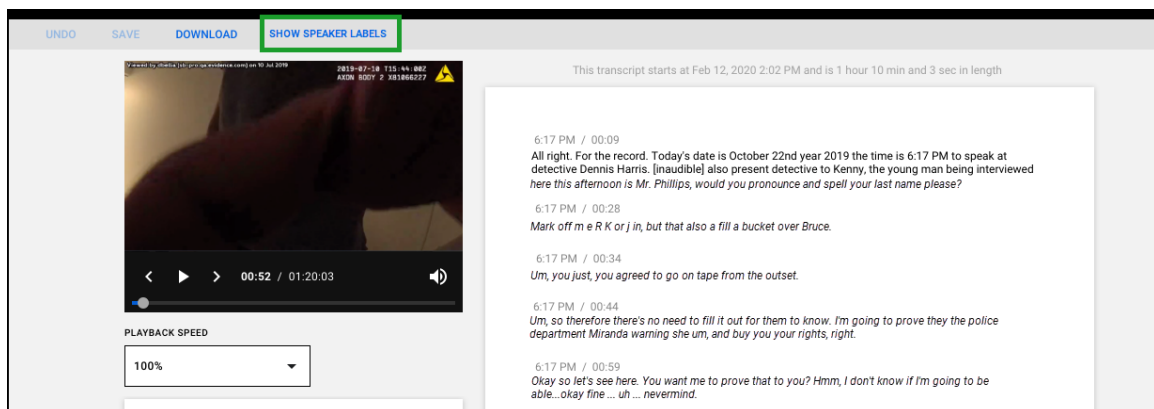
As you type the corrected text, Transcription Assistant looks ahead in the transcript for words that match what you are typing, up to what you've listened to so far. If a word match is found, the words that match are underlined and a gray dashed underline is placed under the text between the matching words. Pressing the **Tab** key will confirm the matching word you are typing and remove the underlined suggestions in between. This allows you to keep listening and confirming text, without worrying about manually removing incorrect suggestions.

Working with Speaker Labels

The initial auto-transcript may be broken into different sections. However, as with speech-to-text, these sections may not be accurate. Transaction Assistant allows you to add new speaker sections, add new speaker labels, and rename the speaker labels.

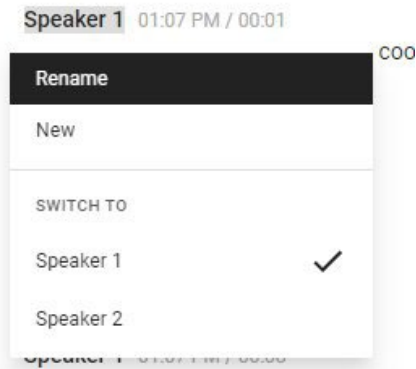
By default, speaker labels are not automatically shown in Fast Evidence Review and Transcription on a completed transcription. If Auto-Transcribe detects a speaker change, it creates a separate block of text.

You can show and edit speaker labels by using the **Show/Hide Speaker Labels** option.



- **Changing Speaker Labels**

In order to change a speaker label, click the speaker label and select the appropriate action.



- **Rename** — This allows you to change the speaker label name and update the other sections with this label to the new name.
Example: If you rename **Speaker 1** to **John Doe**, all **Speaker 1** labels in the transcript are updated to **John Doe**.
- **New** — This adds a new speaker label. This label only affects the current speaker section.
- **Switch to** — This allows you to switch the current speaker label to another existing label by select the label from the list. This only changes the current speaker label. It does not update any other labels.

- **Splitting Speaker Sections**

You can split a speaker section into two sections. To split a speaker section, place your cursor at the point you want the split to occur and press the **Enter** key.

The new speaker section will use the same label as the previous speaker section.

Example: You are splitting a speaker section with label **Speaker 1** and previous section has the label **Speaker 2**. When you split the section, the new section will use the label **Speaker 2**.

- **Merging Speaker Sections**

To merge two speaker sections:

- Place your cursor at the beginning of the section you want to merge and press the **Backspace** key.
OR
- Place your cursor at the end of the section and press the **Delete** key to merge the current section with the next section.

Saving Changes

Transcription Assistant automatically saves your changes every 5 minutes and logs if the transcript was edited in the Evidence and User Audit Trails. You can manually save your changes by:

- Clicking **Save** in the upper left of the Transaction Assistant
- Pressing **Ctrl + S** keys.

You can undo a change by:

- Clicking **Undo** in the upper left of the Transaction Assistant
- Pressing **Ctrl + Z** keys.

You can undo the last 25 changes, even if the transcript was saved.

Downloading a Transcript

You can download a copy of a transcript and set options to customize the appearance of the downloaded transcript from the Transcription Assistant. Currently, the transcript is downloaded as a Word doc (docx) file.

To download the transcript, click **Download** in the upper left of the Transcription Assistant, select the display options for the transcript, and then click **Download**.

Download Transcript

LINE NUMBER FORMAT

Continuous

LINE SPACING

Single space

INDENTATION

No indentation

☒ Show timestamps

☒ Show page numbers

☒ Line break between speakers

☐ Bold speaker names

☐ Colon after speaker names

Change the settings above to customize the transcript format.

CANCEL

DOWNLOAD

The options are:

- **Line Number Format** - Sets the line numbering format in the transcript. The possible selections are No line numbers, Restart on each page, or Continuous.
- **Line spacing** - Sets the amount of space between lines. The possible selections are Single space, 1.5 lines, and Double space.
- **Indentation** - Sets if the transcription text is indented. The possible selections are No indentation, First line, and Hanging.
- **Show timestamps** - When selected, timestamps are shown above the speaker label.
- **Show page numbers** - When selected, a page number is added at the bottom right side of the page.
- **Line break between speakers** - Sets if a line break is included between speakers.
- **Bold speaker names** - When selected, speaker names are shown in bold.
- **Colon after speaker names** - When selected, a colon (:) is added after the speaker name. If **Bold speaker names** is selected, the colon is also in bold.

The following image shows an example of the first page of an unverified downloaded transcript with Line Number Format = Continuous, Line spacing between Speakers = Single Space, Indentation = Hanging, and the Show timestamp and show page numbers options are selected.

Evidence Title: DUI Marijuana.mp4

This transcript is unverified.

An unverified transcript may have been generated through a combination of speech-to-text technology and human edits. As a result, it may contain errors, so please refer to the corresponding evidence.

Last edited by

This transcript starts at Feb 1, 2021 12:28 AM -08:00 and is 32m 24s in length

1 [12:28 AM / 00:24]
 2 **Speaker 1:** <inaudible>
 3
 4 [12:29 AM / 01:00]
 5 **Speaker 2:** Hi. The reason I talked to you is because your registration is expired in August. Were
 6 you aware that the enforcement, sorry, one more second.
 7
 8 [12:29 AM / 01:09]
 9 **Speaker 1:** <inaudible>
 10
 11 [12:29 AM / 01:15]
 12 **Speaker 2:** Sorry. What's that? I had no idea. You had no idea. Okay. Do you have your
 13 registration in the car?
 14
 15 [12:30 AM / 01:44]
 16 **Speaker 1:** Okay. Do you have your insurance in the car? Do you have your current insurance in
 17 the car by chance?
 18
 19 [12:30 AM / 02:07]
 20 **Speaker 2:** Okay. I lose her who's this car belong to. Okay. Gotcha. Um,
 21
 22 [12:30 AM / 02:17]
 23 **Speaker 1:** <inaudible> gotcha. Can you see my bag?
 24
 25 [12:30 AM / 02:27]
 26 **Speaker 2:** Yeah. Can you try and watch it with just your eyes?
 27
 28 [12:31 AM / 02:29]
 29 **Speaker 1:** <inaudible>. So what's your current address?
 30
 31 [12:31 AM / 02:43]
 32 **Speaker 2:** Three 33 Northwest Harrison, three 33 Harrison. Okay. So, uh, have you noticed
 33 when's the last time your car was in the shop?
 34
 35 [12:31 AM / 02:53]
 36 **Speaker 1:** Alright.
 37
 38 [12:31 AM / 02:56]
 39 **Speaker 2:** I left jobs out. Okay. They say anything to you about your shocks? Oh yeah. Yeah,
 40 pretty much. Yeah. You're bouncing your, her with bouncing all over the place on the
 41 road when we were driving down grant, I mean, it was like, it never stopped. It was
 42 just downtown, downtown. Yeah. They did some work on it. It was like a thousand
 43 dollars hundred dollars. You try to have it. Okay. So you said three. Okay. And then
 44 what's your phone number
 45
 46 [12:32 AM / 03:38]
 47 **Speaker 1:** Tonight? All right. Nothing. Nothing at all.

1

Transcript Verification

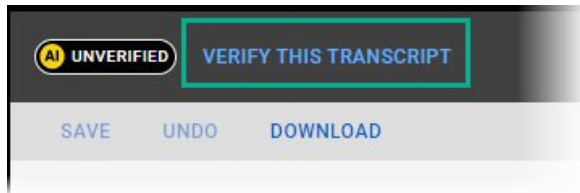
Auto-transcripts are generated using a combination of speech-to-text technology and human input. The transcript can be in one of the following states:

- **Unverified:** An unverified transcript means that it has not yet been marked as verified by a human, and should therefore not be treated as a source of truth. Only while unverified can a transcript can be edited.
- **Verified:** A verified transcript indicates that it has been reviewed and approved by a human. Once a transcript is verified, it is no longer editable. However, users with the

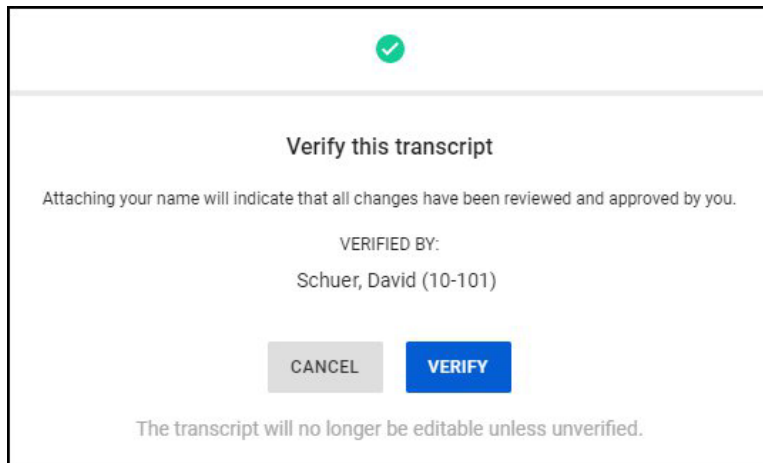
appropriate permissions can change the status to unverified, if edits do need to be made.

Verifying a Transcript

1. Open Transaction Assistant from the Evidence Detail page.
2. Review and confirm the speakers and text in the transcript.
3. When you are ready to verify the transcript, click **Verify This Transcript** in the upper left of the Transcription Assistant.



4. You are asked to confirm that you want to verify the transcript.



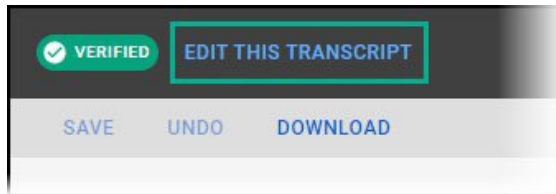
Click **Verify** to continue. The transcription state changes to Verified and the event is recorded in the evidence audit trail.

5. Close Transcription Assistant.

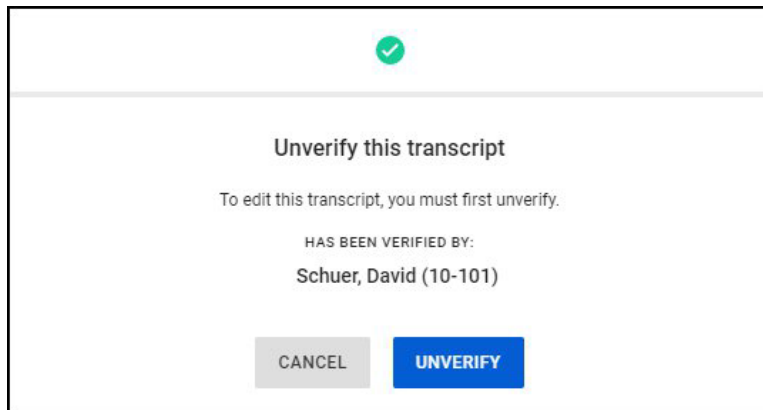
Unverifying a Transcript

In some situations, you may need to unverify a transcript so that it can be edited.

1. Open Transaction Assistant from the Evidence Detail page.
2. Click **Edit This Transcript** in the upper left of the Transcription Assistant.



3. You are asked to confirm that you want to unverify the transcript.



Click **Unverify** to continue. The transcription state changes to Unverified and the event is recorded in the evidence audit trail.

4. Close Transcription Assistant.

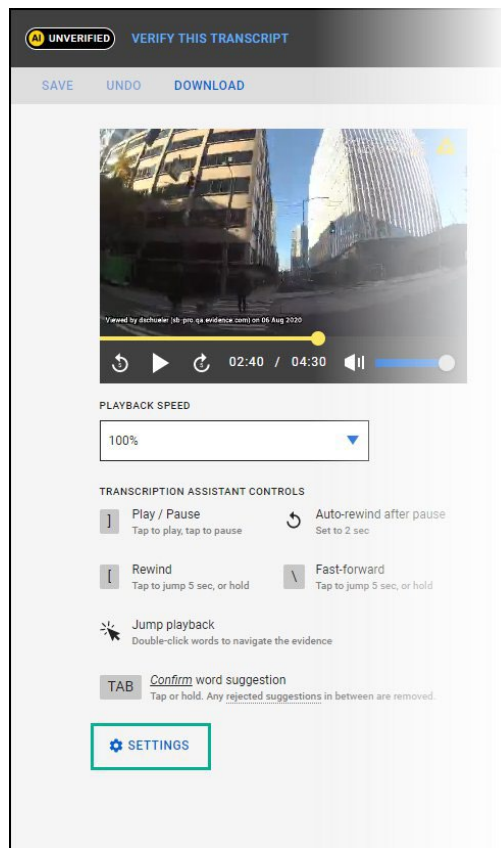
Keyboard Controls

- **Tab** - press to confirm word suggestion. Tap or hold and any rejected suggestions in between are removed.
- **] -** play/pause file playback.
Note: After pausing, the system automatically rewinds the file based on Transcription Assistant Settings (default is 2 seconds).
- **[-** rewind (default is 5 seconds)
- **\ -** fast forward (default is 5 seconds)
- **Ctrl + S** - Save changes
- **Ctrl + Z** - Undo last action

Transcription Assistant Settings

You can change the Transcription Assistant Keyboard Settings to customize the settings for your agency.

1. Open Transcription Assistant.
2. Click **Settings**.



The Control Settings dialog is shown.

3. Select the options for each of the controls.

The screenshot shows a 'Control settings' dialog box with the following options:

- Jump playback:** ☒ Single-click, ☐ Double-click
- Play / Pause:** ☒ Tap to play, ☐ Hold to play
- Rewind:** 5 seconds (dropdown)
- Auto-rewind on pause:** 2 seconds (dropdown)
- Fast-forward:** 5 seconds (dropdown)

A blue **DONE** button is located at the bottom right of the dialog.

- **Jump Playback** – choose controls if Transcription Assistant navigates to the selected point in the transcript and media on a **Single-click** or a **Double-click**.
- **Play/Pause** - choose if you **Tap to play** or **Hold to play** the] key to play the file
- **Rewind** - choose how many seconds file rewinds when the [key is pressed
- **Auto-rewind after pause** - choose how many seconds Transcription Assistant automatically rewinds the file after pausing
- **Fast-forward** - choose how many seconds the file advances when the \ key is pressed

4. Click **Done** to save the settings.

Foot Pedal Support

Foot pedal usage is supported in Transcription Assistant. You must install the Axon Foot Pedal application to use your foot pedal with Transcription Assistant.

1. Download the [Axon Foot Pedal Installation file](#). The Axon Foot Pedal application can be installed on a per-user or per-machine (with administrator rights) basis.
2. Install the file.

Once the Axon Foot Pedal Software is installed and running, your foot pedal controls are mapped to the Transaction Assistant keyboard shortcuts. The center pedal is play/pause, the right pedal is fast forward, and the left pedal is rewind.

Sharing Transcriptions

Transcriptions can be shared inside and outside your agency. This section provides information on how transcripts can be shared.

- **Inside My Agency Sharing**

If a user normally has access to or is added to the access list for a piece of evidence, then they can view that evidence and the associated transcript.

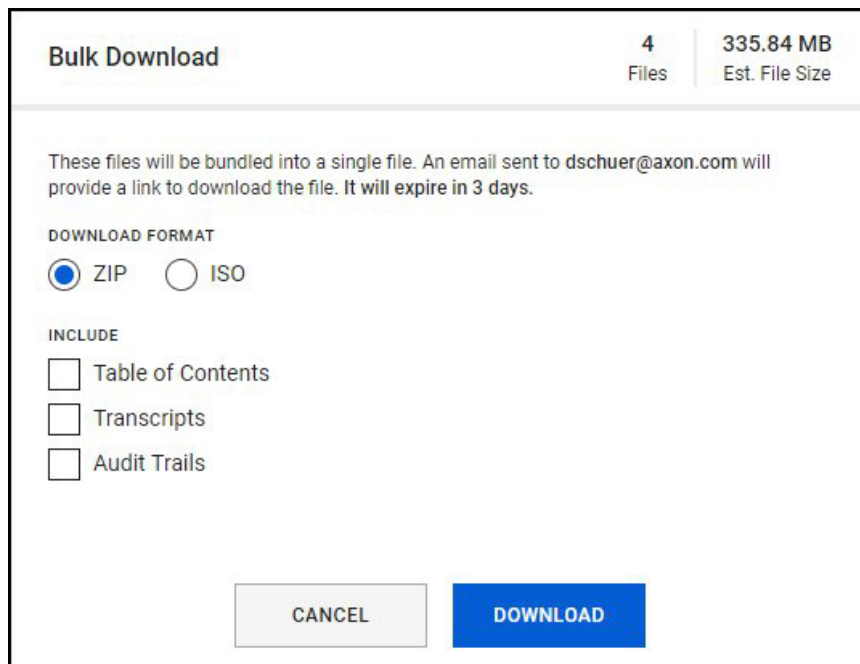
- **Outside My Agency Sharing**

Similar to Inside My agency sharing, if a user is added to the access list for a piece of evidence, then they can view that evidence and the associated transcript.

Similar to other Outside My Agency sharing, users that are not part of an Axon Evidence agency can view evidence through their my.evidence.com account. But they must have an existing account before they are added to the access list.

- **Bulk Download Evidence**

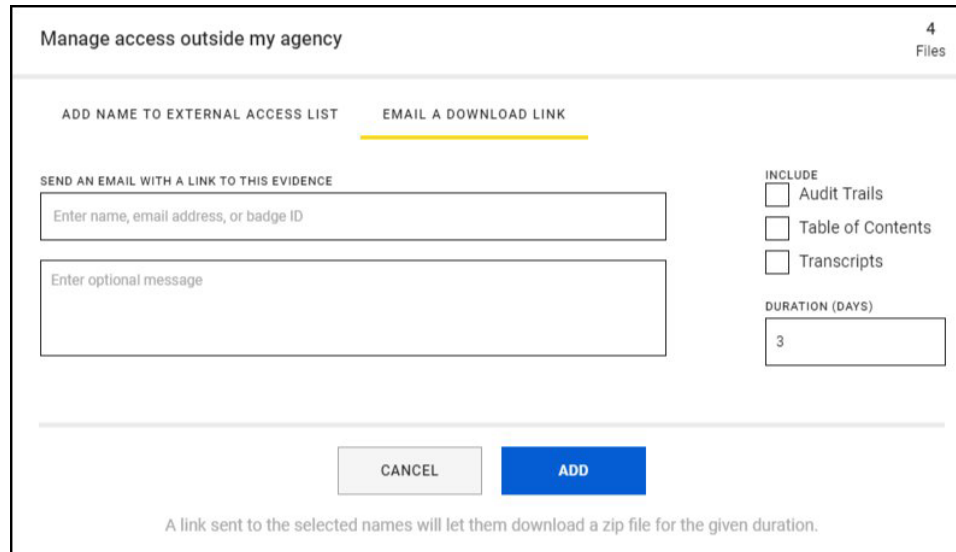
If a user downloads multiple pieces of evidence in bulk, they have the option to include transcripts in the download.



The image shows a 'Bulk Download' dialog box. At the top, it displays 'Bulk Download' on the left, '4 Files' in the middle, and '335.84 MB Est. File Size' on the right. Below this, a message states: 'These files will be bundled into a single file. An email sent to dschuer@axon.com will provide a link to download the file. It will expire in 3 days.' Under the heading 'DOWNLOAD FORMAT', there are two radio buttons: 'ZIP' (which is selected) and 'ISO'. Under the heading 'INCLUDE', there are three checkboxes: 'Table of Contents', 'Transcripts', and 'Audit Trails', all of which are currently unchecked. At the bottom of the dialog, there are two buttons: a grey 'CANCEL' button and a blue 'DOWNLOAD' button.

- **Sharing Outside My Agency by Download Link**

If evidence or a case is shared by emailing a download link, the user has the option to include text file copies of the transcripts.



- **Case Sharing**

- **Inside My Agency Sharing**

If a user normally has access to or is added to the access list for a case, then they can view transcripts associated with evidence in the case.

- **Partner Agency Sharing**

if a user shares a case with a partner agency, they have the option to include transcripts.

Auto-Transcribe Audit Events

The following Auto-Transcribe events are recorded in the Evidence and User Audit Trails.

- Auto-Transcript is Requested
- Evidence Transcript Viewed
- Evidence Transcript Downloaded
- Evidence Transcript Edited

Note: The audit trails only record that editing occurred; the text edits are not recorded in the audit trail.

- Evidence Transcript Deleted
- Evidence Transcript Verified
- Evidence Transcript Unverified

Redaction Studio and Redaction Assistant

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 Assistant is an add-on to the standard Axon Redaction Studio functionality that speeds up your redaction process by checking videos for common objects and automatically adding mask segments to those objects. See [Using Redaction Assistant](#) for more information.

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 object-tracker 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 Microsoft Edge, Firefox, Chrome, and Safari browsers.

Redaction Studio Terms and Concepts

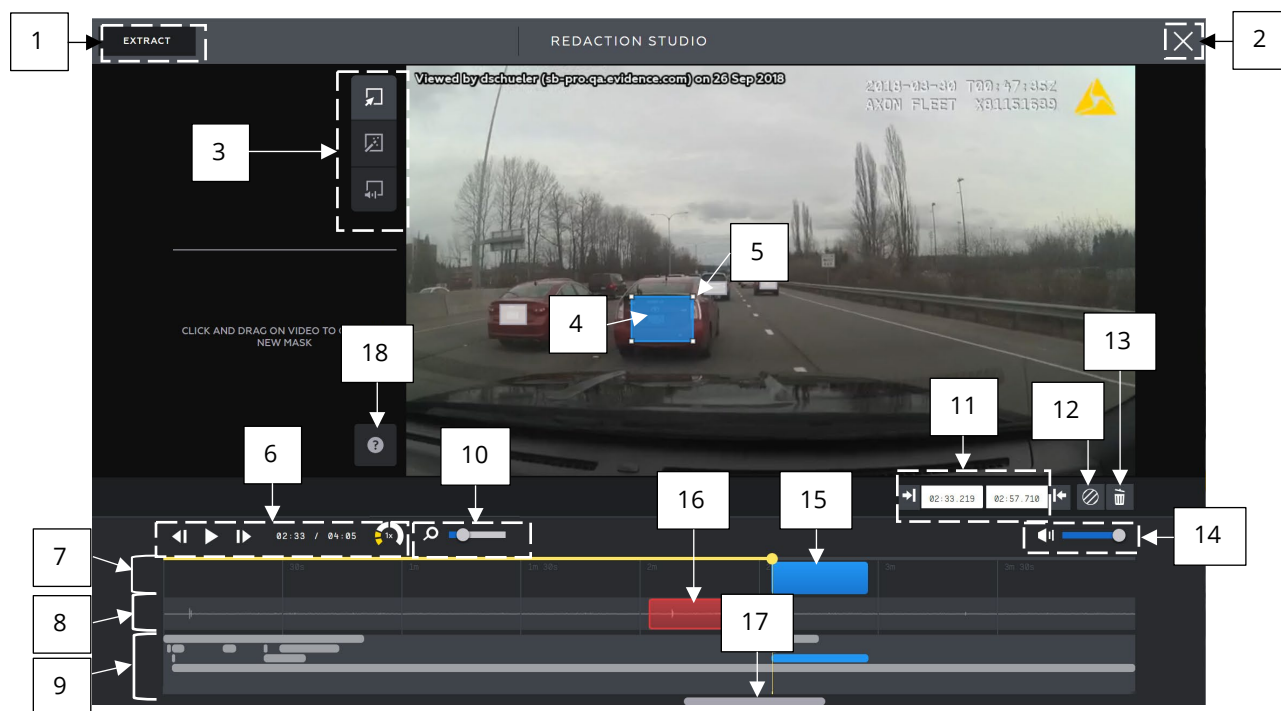
In Evidence.com, *redaction* is a term used to describe the blurring of objects and removal of audio from video evidence. The following terms describe the components in Redaction Studio used to create a redaction:

- **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.

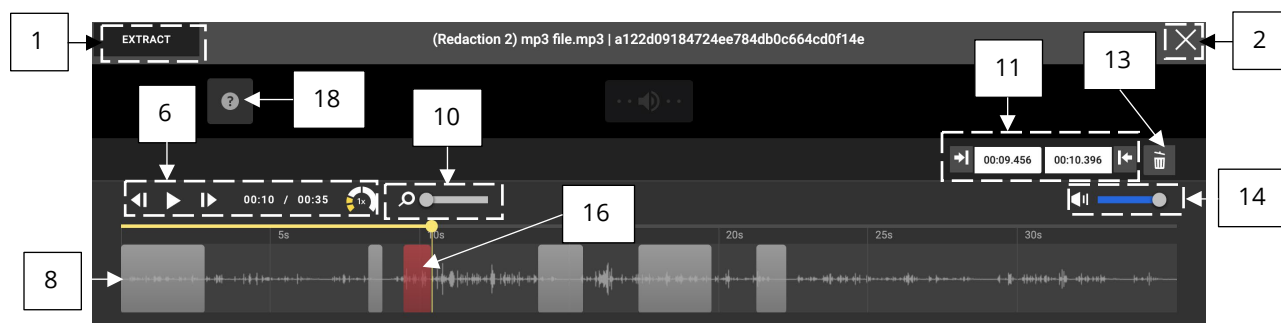
- **Segment Timeline** — The area below the audio track that shows all the video mask segments for the current redaction. This area allows users to easily find and select video masks.
- **Video Mask Frame** — Defines the rectangular area redacted by a mask in a video. Video mask frames can be manually 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 speed, half speed or rewind, 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 five levels of blur and blackout:

	Extra Light blur		Heavy blur
	Light blur		Extra Heavy blur
	Medium blur		Blackout

Redaction Studio Layout and Controls



Video Redaction



Audio Redaction

Redaction Studio 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. Segment Timeline zoom control
11. Start and end times for the selected mask	12. Blur Selector
13. Delete selected mask	14. Playback volume control
15. Video Mask segment for the selected mask	16. Audio Mask segment for the selected mask
17. Segment Timeline scroll bar	18. Show help screen

Keyboard Controls

You can download a PDF file of the Keyboard Controls from the [Axon Help Center Redaction Studio Layout and Controls article](#).

Key	Action
Spacebar	Play/Pause video
1	1x playback speed
2	2x playback speed
4	4x playback speed
D	Forward 1 frame at a time. Hold to play video at half speed.
E	Forward 2 seconds
A	Rewind 1 frame. Hold to rewind video at half speed.
Q	Rewind 2 seconds
W	Increase selected video mask size
S	Decrease selected video mask size
M	Press and hold to place audio mask, release to set end of audio mask.
Del	Delete selected mask from the video frame
Arrow keys (up, down, left, right)	Move selected video mask
[or] (left or right bracket)	Trim mask segment start (left bracket) or end (right bracket) to the current playback time.
+	Zoom in on Segment Timeline
-	Zoom out on Segment Timeline

Note: If the + and - characters on your keyboard layout are combined with another character, you must use the appropriate keyboard combinations to access the + or - character. For example - many keyboards combine + and = on the same key and you must press the Shift and + keys to use the + character.

Redaction Studio Best Practices

The list below has some tips, tricks, and best practices for working with Redaction Studio.

- After processing is complete, Axon recommends that you watch the entire video to verify the video is correctly redacted.
- 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:
 - It is generally easier to redact objects using larger masks.
 - 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.
 - 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.
 - 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 for Video and Audio Redaction

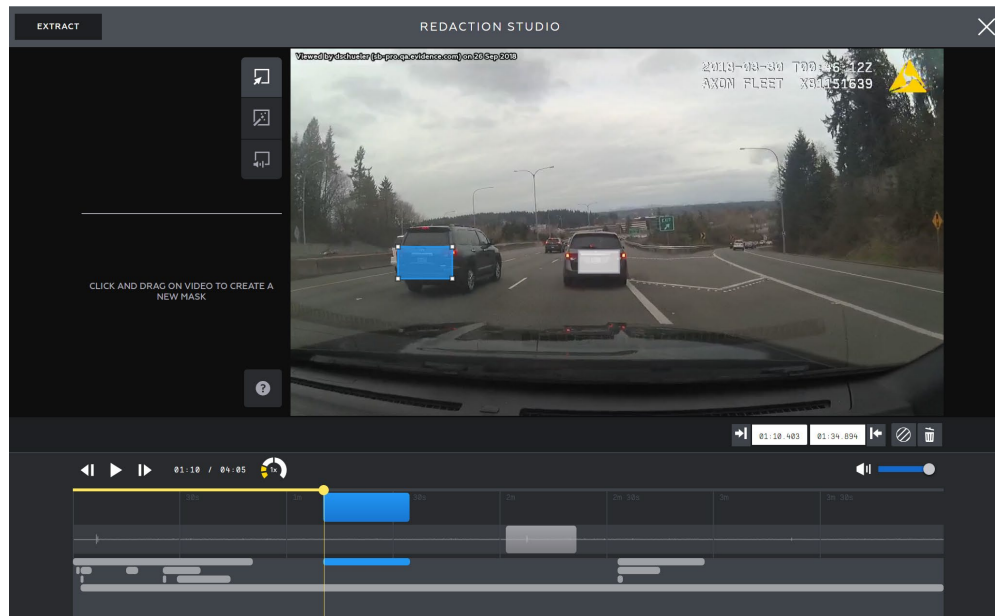
1. On the Evidence Detail page for the evidence you want to redact, below the video player, click **Redactions**.

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 speed, half speed (hold **D** key), rewind 1 frame (**A** key) or rewind half-speed (hold **A** key). 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.

Audio masks can mute the audio or have a one-second bleep sound at the start mask segment.

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.

Action	Method
Add another video mask	<p>It is recommended that you stop video playback before placing new masks.</p> <ul style="list-style-type: none"> • Click on the type of redaction mask you want to use. • Click and drag on the video to place and size the mask.
Add an audio mask:	<p>It is recommended that you stop video playback before placing new masks.</p> <ul style="list-style-type: none"> • Click on the Audio redaction mask. • Click on the Audio Track to place. • Set the length of the mask.

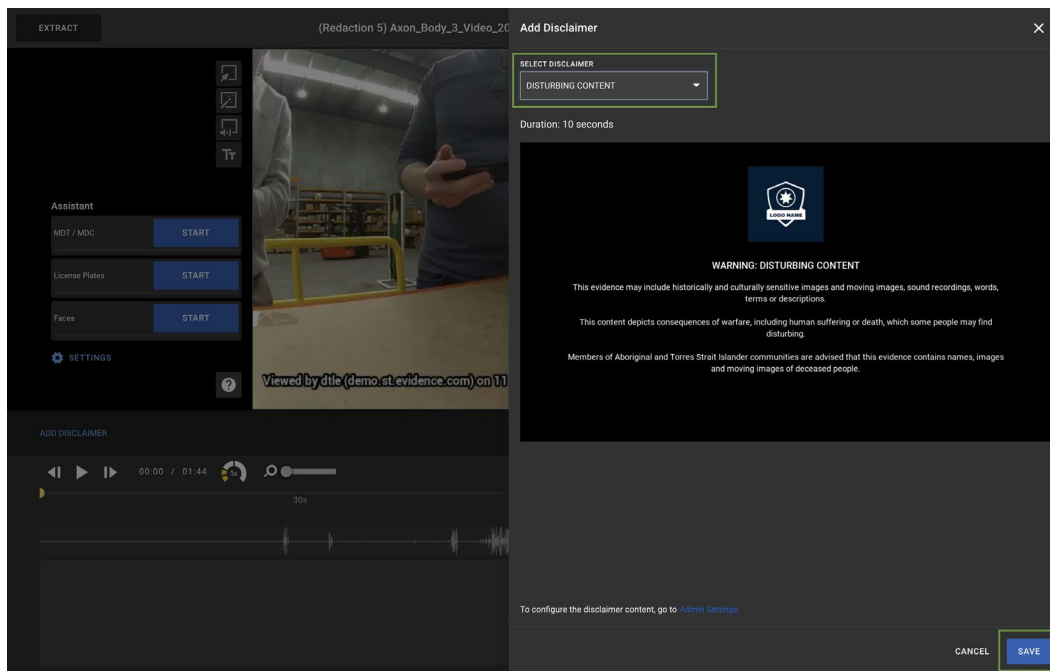
Action	Method
Add bleep sound to an audio mask:	<p>This action can be done while adding the audio mask.</p> <ul style="list-style-type: none"> Select the audio mask. In the audio mask sound list, select Short bleep. This adds a one-second bleep sound at the start mask segment. The bleep can be removed by selecting Mute on the audio mask sound list.
Delete a mask	<ul style="list-style-type: none"> Click the mask you want to delete. The selected mask changes color, based on the redaction type (blue for manual, green for tracking). Click the delete icon.
Move a video mask	<ul style="list-style-type: none"> Click the mask you want to move. The selected mask changes color, based on the redaction type (blue for manual, green for tracking). Use the arrow keys to move the mask OR Move the cursor over the mask until it turns into a four-arrow pointer. Click and hold to drag the mask to where you want it. Release the mouse button.
Change the size of a video mask	<ul style="list-style-type: none"> Click the mask you want to resize. The selected mask changes color, based on the redaction type (blue for manual, green for tracking). Use the W (increase) or S (decrease) keys to change the size. OR Move the cursor over a corner of the mask until it turns into a double-headed-arrow pointer. Click and hold to drag the corner to resize the mask. Release the mouse button.
Change the blur level of a video mask segment	<ul style="list-style-type: none"> Click the mask. The selected mask changes color, based on the redaction type (blue for manual, green for tracking). Click the Blur Selector until the blur level you want is selected. You can select Light, Medium, Heavy, or Blackout.

Action	Method
Play faster or slower	<ul style="list-style-type: none"> Click the playback speed selector until the speed you want is selected. You can choose from half speed (0.5), standard speed (1X), double speed (2X), or quadruple speed (4X).
Zoom in or out on the Segment Timeline	<p>The maximum zoom in will show a 10 second view of the segment timeline and the maximum zoom out will show a 3-minute view of the segment timeline. Use the scroll bar below the segment timeline to scroll to different parts of the segment timeline while zoomed in.</p> <ul style="list-style-type: none"> Click and hold the zoom slider to zoom in or out. Press the + key to zoom in on the segment timeline and the - key to zoom out. <p>Note: If the + and - characters on your keyboard layout are combined with another character, you must use the appropriate keyboard combinations to access the + or - character. For example - many keyboards combine + and = on the same key and you must press the Shift and + keys to use the + character.</p>
Adjust the start or end point for a mask segment.	<p>Note: The bracket keys ([or]) can be used to trim a mask segment to the current</p> <ul style="list-style-type: none"> Click the mask. The selected mask changes color, based on the redaction type (blue for manual, green for tracking, red for audio). 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 pointer. Drag the segment left or right, as needed. Release the mouse button.
Adjust mask segment start or end point to a specific time	<ul style="list-style-type: none"> Click the mask. The selected mask changes color, based on the redaction type (blue for manual, green for tracking, red for audio). In the Start box, enter the exact time in minutes and seconds, in <i>mm:ss</i> format, where you want the mask segment to start. In the End box, enter the exact time in minutes and seconds, in <i>mm:ss</i> format, where you want the mask segment to end.

- Optionally, click **Add Disclaimer** to add an agency disclaimer to the start of the redacted video.

Use the Select Disclaimer list to choose the appropriate disclaimer. When selected, the disclaimer and duration time are shown in the panel.

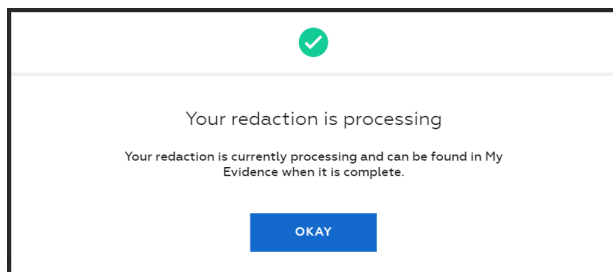
Click **Save** to add the disclaimer.



- When you have finished adding and configuring all the masks, click **Extract**.

Select **Extract Video** and 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.

After processing is complete, Axon recommends that you watch the entire video to verify the video is correctly redacted.

7. 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.

Using Redaction Studio for Audio Extracts

The Audio Extraction functionality lets you extract a redaction as audio evidence in mp3 format with no associate video.

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.

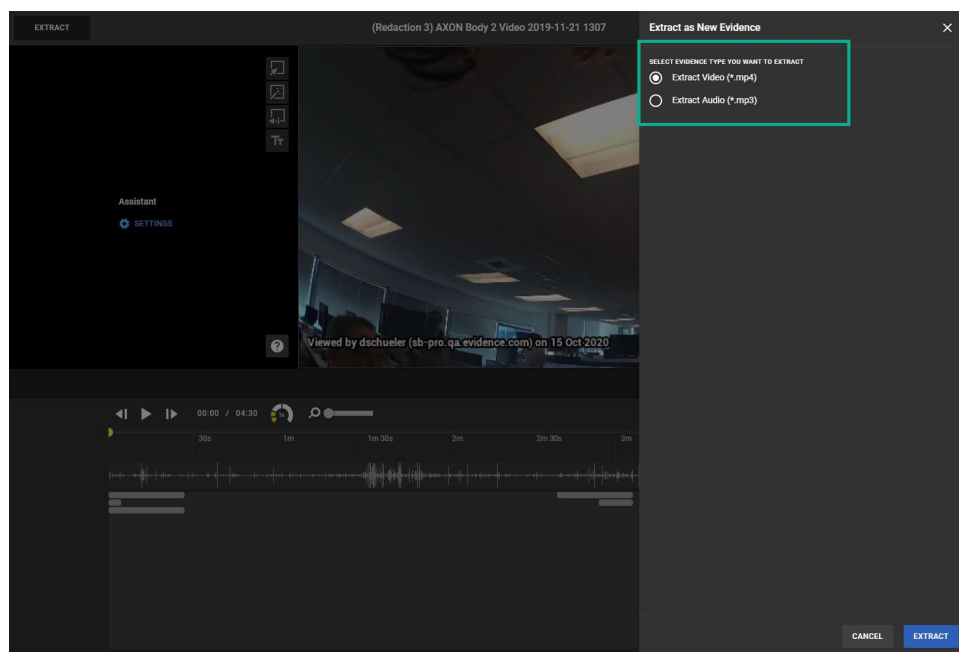
2. Click **Redaction Studio**.

This launches Redaction Studio within the browser window.

3. Click **Extract**.

Select **Extract Audio** and 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 audio file.

4. 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.

Using Redaction Studio for PDF Document Redaction

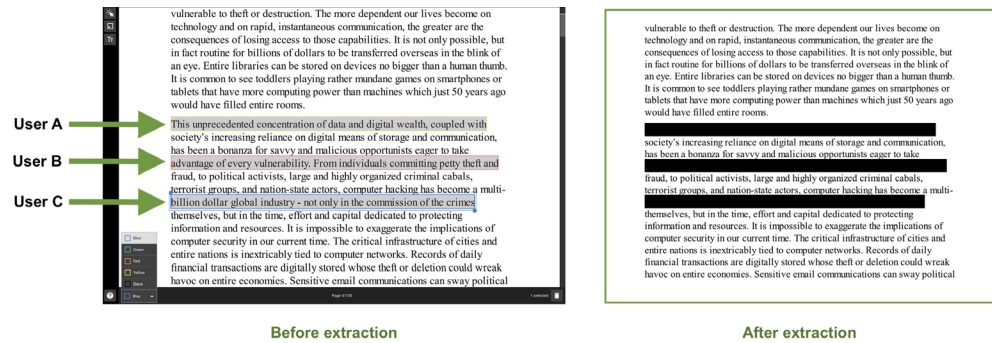
Document Redaction adds the ability to redact text, highlight text, and add text annotation to PDFs in Axon Evidence.

Document Redaction Best Practices

- **Password Protected Documents:** Redaction Studio currently does not support password-protected PDF documents. To redact a document, password protection must be removed before opening the document in Redaction Studio.
- **File Size:** Document Redaction does not have a file size limit. However, works with PDF documents of up to 800 pages. However, documents that contain images or other memory-intensive data load slowly. PDF documents with more than 800 pages are not limited but may cause lagging experience.
- **Hyperlinks:** While a document is open in Redaction Studio, external hyperlinks in the document are disabled. This was done to prevent accidental access to external content while redacting. However, those hyperlinks are preserved after extraction and can access external content while being viewed on the Evidence Detail page. Hyperlinks that go to a point within the document are not disabled while in Redaction Studio.
- **Multi-user Collaboration:** Document Redaction currently allows multiple users to access and work on the same document at the same time. However, as work conflicts can cause undesirable effects when many changes happening in the same place, it is recommended that users do not work in the same areas to reduce overlapping edits.

If in doubt or if Redaction Studio informs you of conflicting changes, refresh the browser page to see the latest changes.

Additionally, users can select different mask border colors to distinguish between their work to avoid overlapping. Mask color settings do not affect the mask appearance after extraction.



- Mask and Annotation Usage:** Only use the redaction mask tool for redacting and annotation for marking or leaving notes. While annotation text with a solid background appears to mask text in a document, it is not as secure as redaction done with the Text Selection tool mask or Mask tool and can be reversed to reveal the content. Users should take caution not to use the Annotation tool as a replacement for a redaction mask.
- Page Navigation:** The scrollbar on the right side of the page provides yellow marks to show where masks or annotations are placed in the document. Click on the scrollbar or move the cursor to jump to a mask or annotation in the document.
- Keyboard Controls:** The following keyboard controls can be used with document redaction. You can download a PDF file of the Keyboard Controls from the Axon Evidence product guide page (link coming soon) on My Axon.

[Keyboard Shortcuts - Document Redaction.pdf](#)

Key	Action
V	Selection tool
M	Mask tool
T	Annotation tool
W	Increase selected mask size
S	Decrease selected mask size
Del	Delete selected mask
Arrow keys (up, down, left, right)	Move selected mask
Crtl/Cmd+F	Open search (Redaction Assistant only)

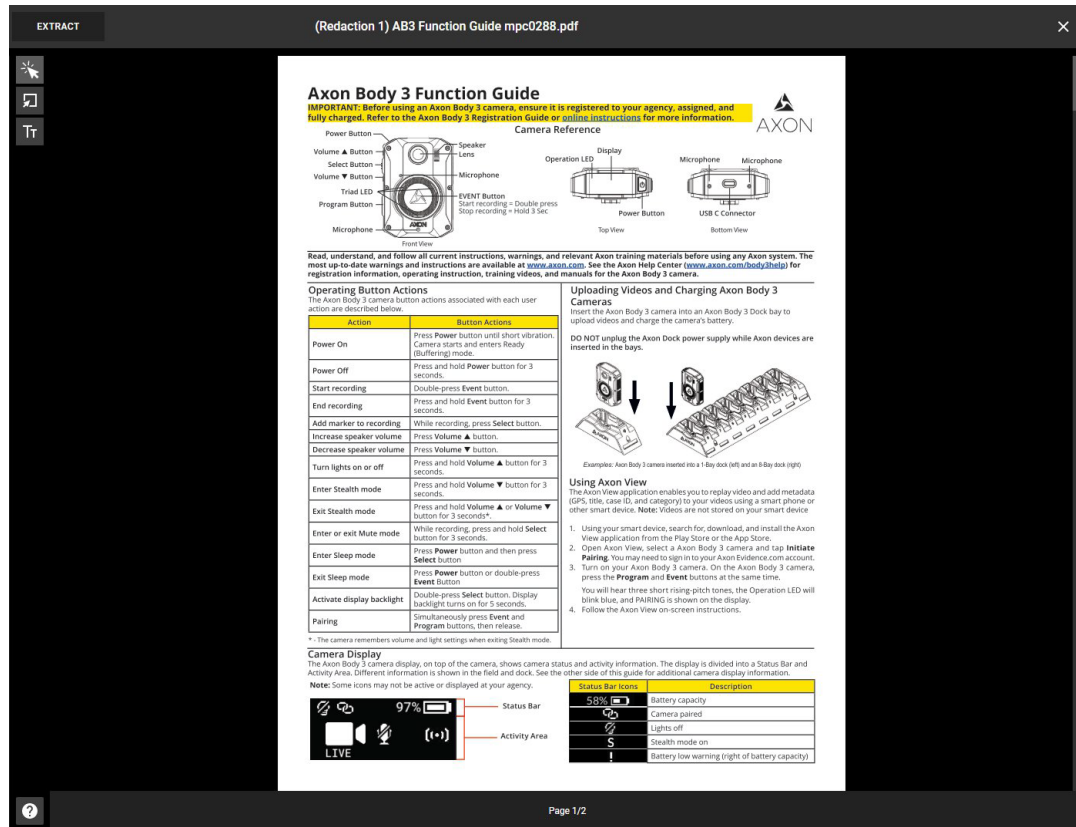
Redacting a PDF Document

- On the Evidence Detail page for the PDF evidence you want to redact, click **Redactions** below the evidence display.

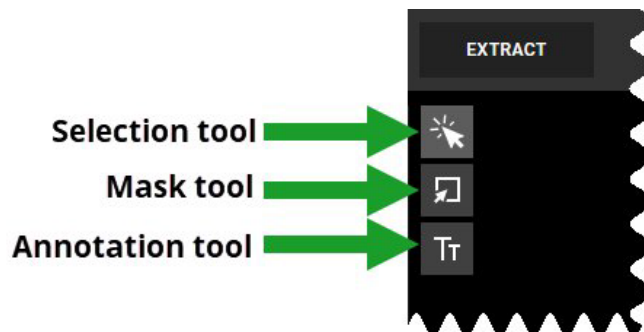
The Redaction Studio and Redaction Tools buttons appear below the Redactions tab. If any redactions already exist, they are listed below the buttons.

2. Click Redaction Studio.

This launches Redaction Studio within the browser window.



3. Select the tool you want to use and add masks and annotations as needed to the document.



- **Selection tool:** This tool lets you use your mouse to select text in the document and then create a mask over the text or highlight the text.

Select the text you want to redact or highlight and select **Create Mask** or **Create Highlight**.

You can select the color associated with your work. Text is hidden by masks and the mask will be black after extraction. The mask color (black, yellow, green, blue, or red) can be used during redaction to indicate work by different users or differentiate subjects. Text is visible through a highlight and the selected color (green, blue, or red) is the highlight color after extraction.

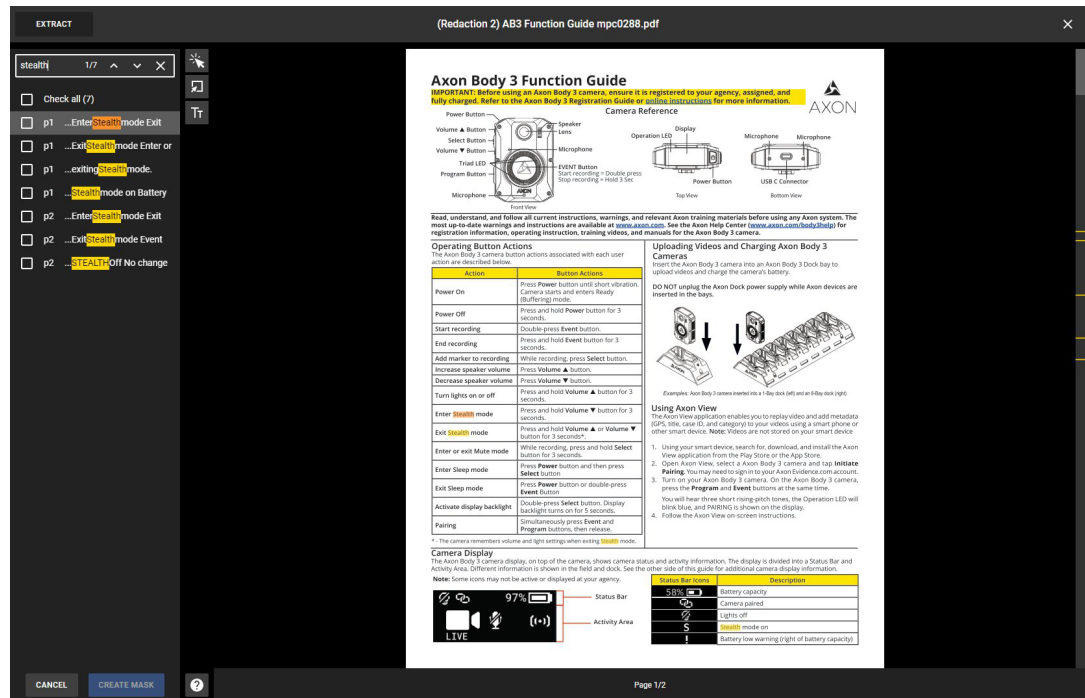
The Selection tool can also be used to select multiple mask, highlight, and annotation text boxes by clicking on the first box and then holding the **Ctrl** or **Cmd** key and then selecting the other text boxes.

- **Mask tool:** This tool lets you use your mouse to select an area in the document and then create a mask over the area. Click and hold on a location in the document and then drag your cursor to create the mask. While a mask is selected, you can change the mask size and location. Text and images are hidden by masks and the mask will be black after extraction. The mask color (black, yellow, green, blue, or red) can be used during redaction to indicate work by different users.
- **Annotation tool:** This tool lets you add text annotation to the document. Click on a location on the document and type the annotation text. You can select a background color and text color for the annotation, along with using the slide bar to set the text size.

Note that annotation is not redaction. While annotation text with a solid background appears to mask text in a document, it is not as secure as redaction done with the Text Selection tool mask or Mask tool and can be reversed to reveal the content. Users should take caution not to use the Annotation tool as a replacement for a redaction mask.

- **Redaction Assistant Search:** Redaction Assistant users have access to the search and redact functionality. This allows you to search for keywords in the document and create masks in bulk.

The search feature also supports jumping to search result to preview.



4. When you have finished adding and configuring all the masks, click **Extract**.

The media processing dialog box is displayed. Click **OK** to continue.

Redaction Studio begins processing the redaction. When processing is complete, Axon Evidence sends an email notification with a link to the redacted document.

After processing is complete, Axon recommends that you watch the review the document to verify the video is correctly redacted.

Using Redaction Studio Annotation Tools

The Redaction Studio annotation tools allow users to add outline markers and text to a video redaction. The annotation tools can be used while doing a normal redaction in Redaction Studio.

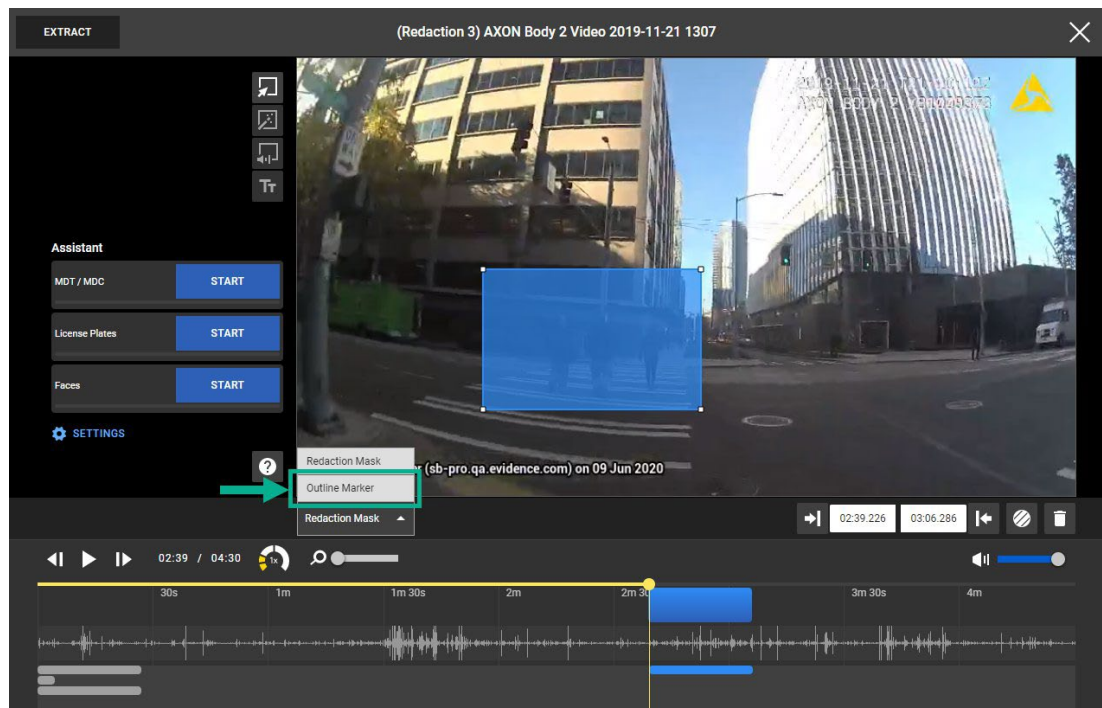
Outline markers are boxes that can be placed over objects to highlight them in the video. Outline markers can be moved during the video, allowing them to follow the object. The workflow for adding an outline marker is similar to using manual mask or object tracker mask.

The text tool allows users to place text in the video. After being placed, the text box can be moved to improve the placement, but cannot change position when the video is played.

Adding an Outline Marker

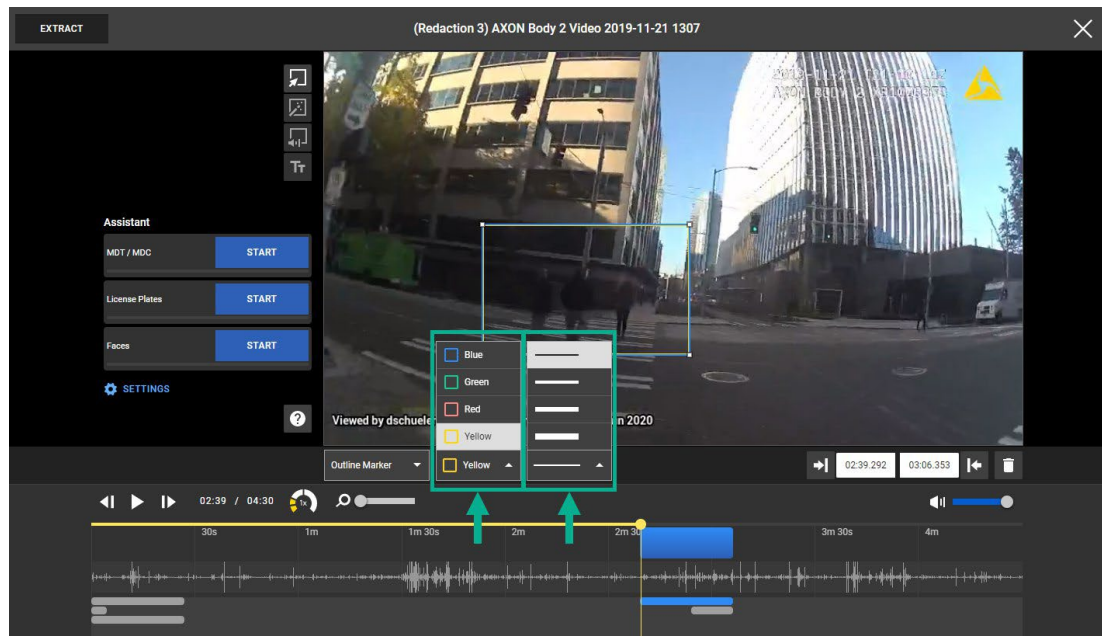
From Redaction Studio:

1. Select the type of redaction mask (manual or object tracker) you want to use as an outline marker.
2. Click and drag on the video to place and size the mask
3. Click the Redaction Mask selector under the video and select **Outline Marker**.



The mask will change from a filled in mask to an outline.

4. After selecting Outline Marker, you can change the outline marker color and thickness using the selectors.



5. Your next action depends on the type of mask you selected as the basis for the outline marker:

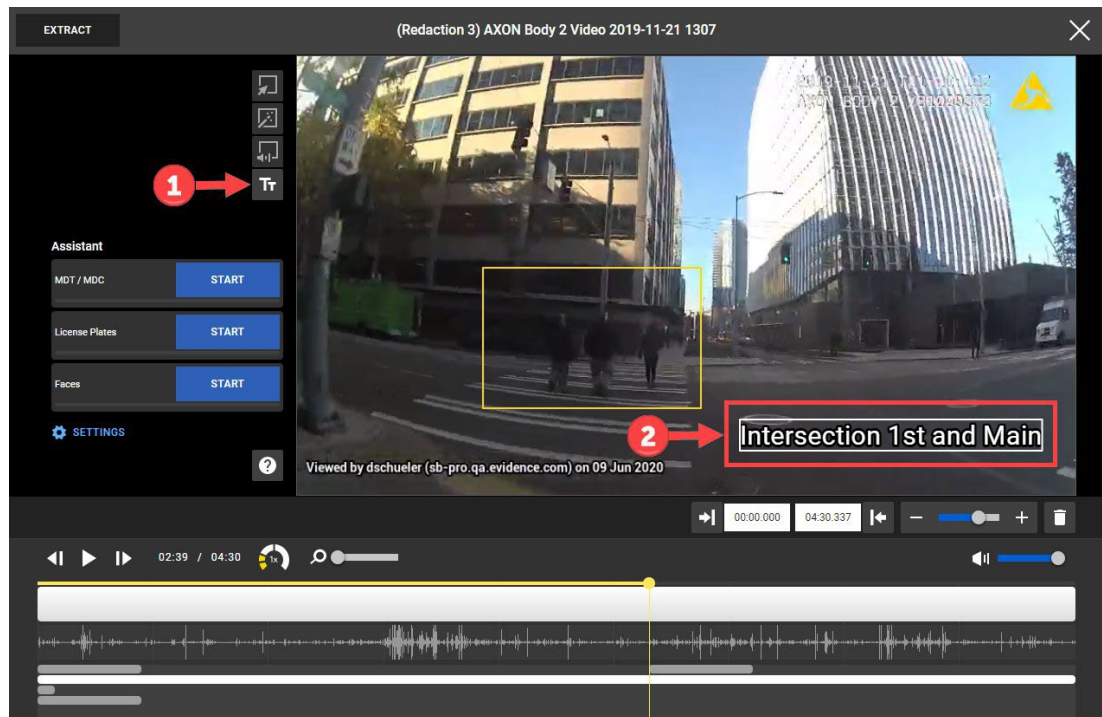
Note: The standard Redaction Studio keyboard controls can be used when working with outline markers.

- If you selected a manual mask for the outline marker, you will be able to manually move and resize the outline marker as needed.
 - If you selected an object tracker mask for the outline marker, it will begin processing to follow the object. You can adjust the size and location as needed to follow the object.
6. Repeat the above steps to place additional outline markers.
 7. Complete the redaction as needed. When you have finished adding and configuring all the masks markers and text, click **Extract**.

Adding a Text Box

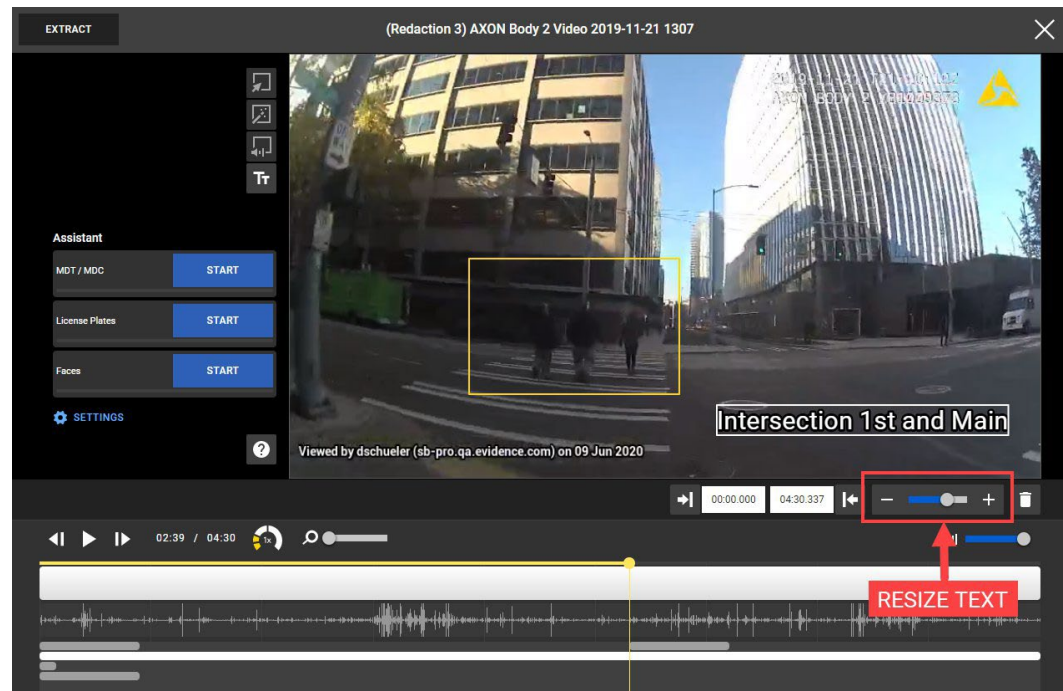
From Redaction Studio:

1. Click the Text icon
2. Click in the video and begin typing or paste the text you want on the redaction.



3. To change the size of the text or move the text box:

- Click on the text to select the text box. A white outline shows the box is selected.
- Click and hold on the text box outline and then move your mouse to reposition the text box.
- To change the size of the text, use the slider bar under the video to increase or decrease the text size.



- Double-click in the text box to change or add more text to the box.
4. Repeat the above steps to place additional text boxes.
 5. Complete the redaction as needed. When you have finished adding and configuring all the masks markers and text, click **Extract**.

Using Redaction Studio for Image Redaction

Currently, image redaction only supports .jpg and .png file types. Support for other file types will be added in future releases.

1. On the Evidence Detail page for the evidence you want to redact, below the image, 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**.

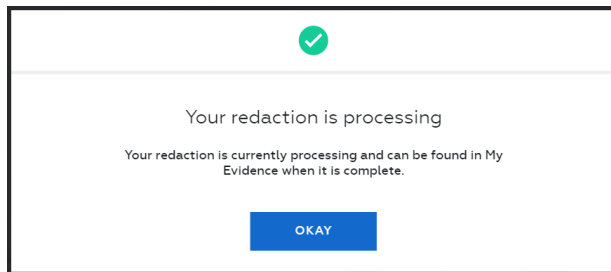
This launches Redaction Studio within the browser window.

3. If needed, the image can be rotated before and while adding masks.
4. Place the cursor on the image, then click and drag to add a mask.

Once a mask is added, the size of the mask can be adjusted with the mask frame handles or by using the W (increase size) or S (decrease size) keys. To move a mask click and hold on the mask and then drag it to the correct location or use the arrow keys to move it.

5. Set the mask blur level as needed. With the mask selected, click on the blur level to cycle between light, medium, heavy, and blackout blur levels.
6. 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 image.

7. Click **X** to exit Redaction Studio and return to the Evidence Detail page.

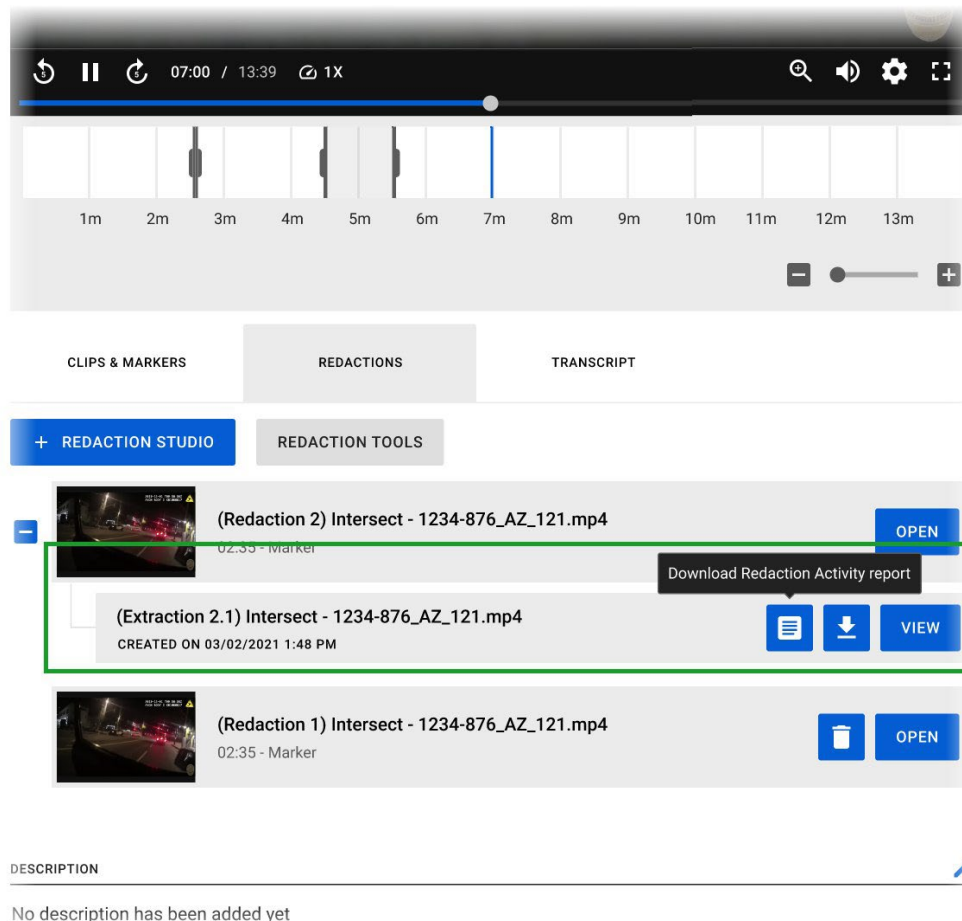
Note: All work done to a video in Redaction Studio is saved.

Redaction Activity Report

The Redaction Activity Report lists the objects (audio and video masks, outlines, and text) added by Redaction Assistant and Redaction Studio. The report is viewed and downloaded from the Redactions tab on the Evidence Detail Page of the original evidence.

1. Open the Evidence Detail page for the original evidence.
2. Click the **Redaction Studio** tab.
3. Click the **+** icon to the right of the redaction with the report you want to download. This expands the redaction information shown.

4. Click the Download Redaction Activity Report icon.



The screenshot displays the Axon Evidence interface. At the top is a video player with a timeline from 1m to 13m. Below the player are three tabs: CLIPS & MARKERS, REDACTIONS, and TRANSCRIPT. The REDACTIONS tab is selected. Under this tab, there are two main sections: 'REDACTION STUDIO' and 'REDACTION TOOLS'. The 'REDACTION STUDIO' section shows a list of redaction items. A green box highlights the 'Download Redaction Activity report' button, which is represented by a document icon with a download arrow. Other buttons like 'OPEN', 'VIEW', and 'DELETE' are also visible for each redaction item.

DESCRIPTION

No description has been added yet

The downloaded report is in a .csv file format. Each line in the report shows the object type and the start and end time for each different redaction object.

Note: if a disclaimer is added to the redaction, the timestamp information is adjusted based on the length of the disclaimer.

No	Type	Timestamp
1	Disclaimer	00:00:00 - 00:10:00
2	Video Redaction (Object Tracker)	00:10:00 - 00:15:12
3	Audio Redaction (Beep)	00:15:23 - 00:15:30
4	Audio Redaction (Mute)	00:15:40 - 00:15:45
5	Video Redaction (Assistant - Face)	00:16:00 - 00:17:15
6	Video Redaction (Assistant - MDT/MDC)	00:18:00 - 00:23:31
7	Adding Text	00:19:11 - 00:20:13
8	Adding Outline marker	00:19:16 - 00:20:13
9	Video Redaction (Manual)	00:20:23 - 00:25:12

Using Redaction Assistant

Redaction Assistant speeds up your redaction process by checking videos for common objects, such as license plates, MDT/MDC screens and faces, and automatically adding mask segments to those objects. This cuts down the amount of time you need to spend on tedious, repetitive tasks and allows you to focus on more important parts of redaction. Additionally, Redaction Assistant's ability to identify objects will improve over time, further reducing the time needed for reviewing and editing.

Redaction Assistant is an add-on to the standard Axon Redaction Studio functionality and may not be available at your agency.

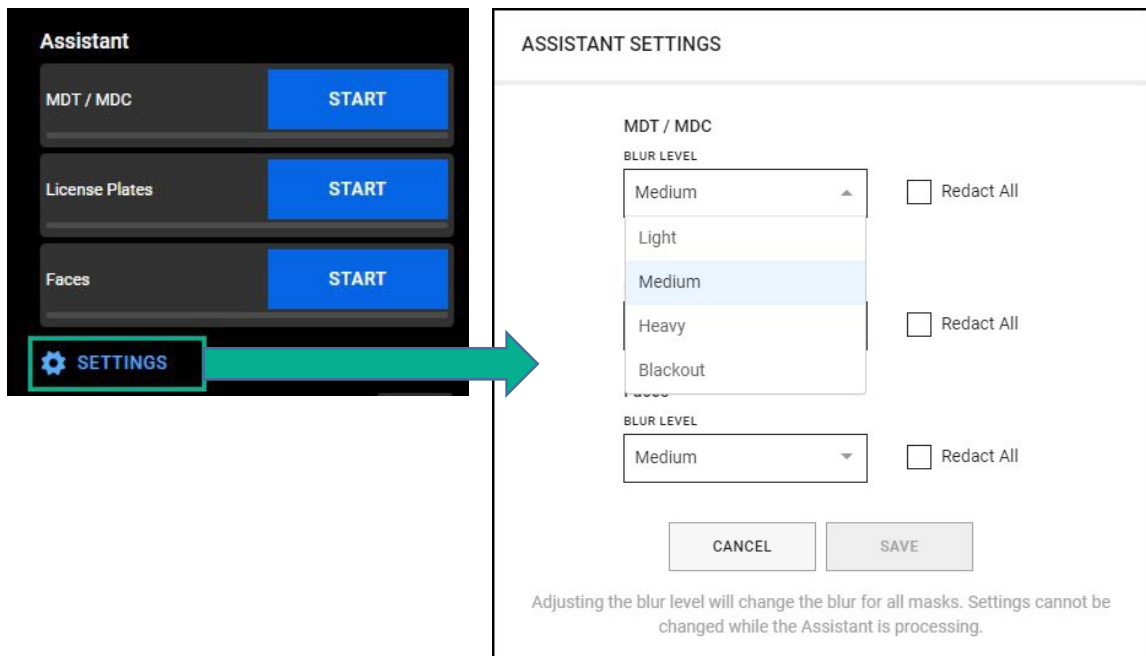
Note: Redaction Assistant can only process 15 masks for faces at the same time. All detected faces will be masked, but they may not all be processed at the same time. In some situations, it may appear that Redaction Assistant is not processing all object. If this happens, Axon recommends waiting until Redaction Assistant completes processing for all the selected objects before adding your own masks to those objects.

For example, if Redaction Assistant detects 16 faces in a video, it will process the initial 15 masks first. The 16th face mask is placed in a waiting queue until one other mask finishes processing and then it will be processed.

Redaction Assistant Settings

The Redaction Assistant settings allow you to configure your own default settings for Redaction Assistant masks. The settings can be changed before or after starting Redaction Assistant or while reviewing the redaction. This way you can customize Redaction Assistant on the fly, providing you with flexibility and time-savings in your redaction work.

This functionality is accessed by clicking Settings under the Assistant section in Redaction Studio.



From there you can set if the Redact check boxes for Redaction Assistant masks are selected or not, and set the blur level for each process. Once saved, the settings will apply to all Redaction Assistant masks until you change them.

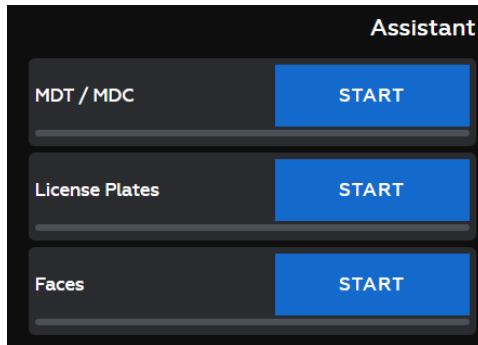
For example, if you are redacting a video where you need to blur all but a few faces, you can change the Redaction Assistant setting for Faces by selecting Redact All (as shown in the image below) so the Redact check box for Faces masks are selected and then you only need to clear a few masks. Alternately, if you have video where you only need to blur a few people, you can change the setting, so the mask Redact check box is cleared, and then select the few faces you want to redact.

Starting Redaction Assistant

1. On the Evidence Detail page for the evidence you want to redact, below the video player, click **Redactions**.
2. Click **Redaction Studio**.

This launches Redaction Studio within the browser window.

3. Click **Start** for the Redaction Assistant processes you want to use on the video.



Note: Redaction Assistant uses the same blur level as the last redaction mask you used. If you want Redaction Assistant to use a different blur level, then before you start a scan - add a video mask with the appropriate blur level, delete the mask, and then start the Redaction Assistant scan.

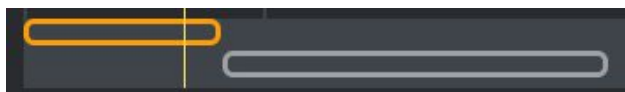
- **MDT/MDC:** This process checks the video for vehicle MDT/MDC screens and adds masks to cover the screens.
- **License Plates:** This process checks the video for vehicle license plates and adds masks to cover the plate.
- **Faces:** This process checks the video for faces and adds masks to cover the faces, and then provides users with the option to choose which individual faces to redact.

Note: Redaction Assistant can only process 15 masks for faces at the same time. All detected faces will be masked, but they may not all be processed at the same time. In some situations, it may appear that Redaction Assistant is not processing all object. If this happens, Axon recommends waiting until Redaction Assistant completes processing for all the selected objects before adding your own masks to those objects.

For example, if Redaction Assistant detects 16 faces in a video, it will process the initial 15 masks first. The 16th face mask is placed in a waiting queue until one other mask finishes processing and then it will be processed.

Redaction Assistant begins scanning and processing the video.

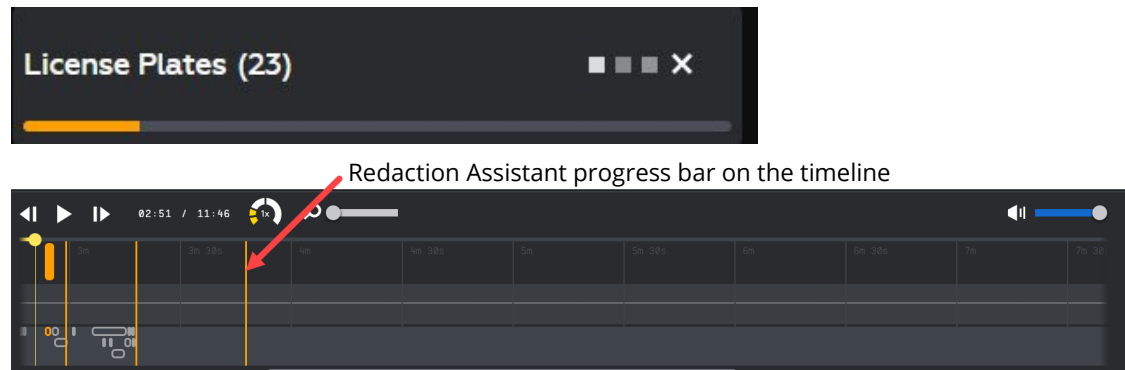
Masks initially appear as open rectangles in the segment timeline. This allows the user to view and confirm that the object should be redacted. Once the mask for an object is confirmed, the segment timeline rectangle will be filled.



While Redaction Assistant is processing, you can continue redaction work on the video and even adjust Redaction Assistant masks. You can also exit Redaction Studio and Redaction Assistant will continue to scan and process the video.

A Redaction Assistant progress bar shows the status of the redaction check. When the progress bar shows the check is complete, you can review the all masks added by Redaction Assistant.

The following images show the progress bar appearance during a scan.



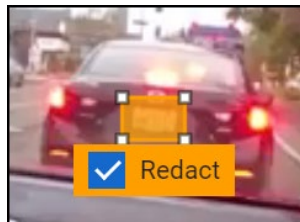
Reviewing Redaction Assistant Masks

After the Redaction Assistant places a mask, you can review and edit the mask.

Axon recommends that you watch the entire video to verify that masks were added to all the appropriate objects.

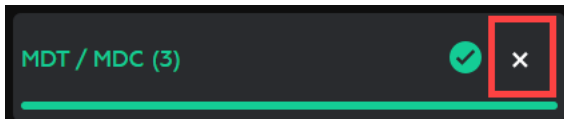
Redaction Assistant masks are orange when selected on the video or segment timeline. Redaction Assistant masks are automatically selected to be redacted with the extraction. The mask must be manually excluded if it should not be part of the redaction.

To review a mask:



- Select the mask in the segment timeline.
- Review the mask. If the object should not be redacted, then clear the **Redact** check box.
- You can adjust the mask as needed.

You can delete all the masks of a certain type by clicking the **X** on the appropriate process bar.



When working with Redaction Assistant masks you can:

- Adjust the start and end times for the mask
- Change the blur level of the mask
- Delete a mask
- Move and change the size of a mask
- Use Spray Paint Redaction with Redaction Assistant masks to extend segments with finer control. Just click and hold on the mask during video playback at normal, half speed, or rewind, and then use your mouse to follow the object you want to redact.

Once you have reviewed and edited the Redaction Assistant masks and added any of your own masks, you can extract the video normally.

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.

Creating a Case

Cases can be created by administrators and users who have the necessary permission settings. For more information about role-based permissions, contact your administrator.

The Add Suggested Evidence feature makes it easy to add evidence to a case while you are creating the case. The feature finds any evidence files that include the ID you search for. For example, if you search for 345, the results would include the evidence file IDs 12345 and 76345.

1. On the menu bar, click **Cases** and then, below the search filters, click **Create Case**.

The Create Case page appears.

2. Enter a Case ID, using the format set by your agency.

If any evidence in your agency contains the ID entered into the case ID field, you will receive a message telling you how many pieces of matching evidence were found.

If any cases in your agency have the same ID that was entered into the case ID field, you will receive a message telling you that another case has the same ID. However, you can create a case with the same ID as another case.

3. Enter an optional description, then click **Select Evidence**.

Evidence.com searches for evidence files that contain the same ID as the ID you used for the case and lists them as suggested evidence. If no evidence is suggested, you can search for evidence files. For more information, see [Text Search Details](#).

The Select Evidence page lists 100 evidence files at a time. You can add multiple files to a case at one time. To select all of the evidence on the page, select the check box at the top of the list. If more than 100 evidence files are listed, you can select 100 at a time and click **Next** to view the next set of files.

4. On the Select page, select the check box to the left of the evidence, then click **Add to Case** or **Review**.
 - **Add to Case** lets you add the selected evidence to the case without reviewing it. Once evidence is added to the case, you can click **View Case Evidence** to see the list

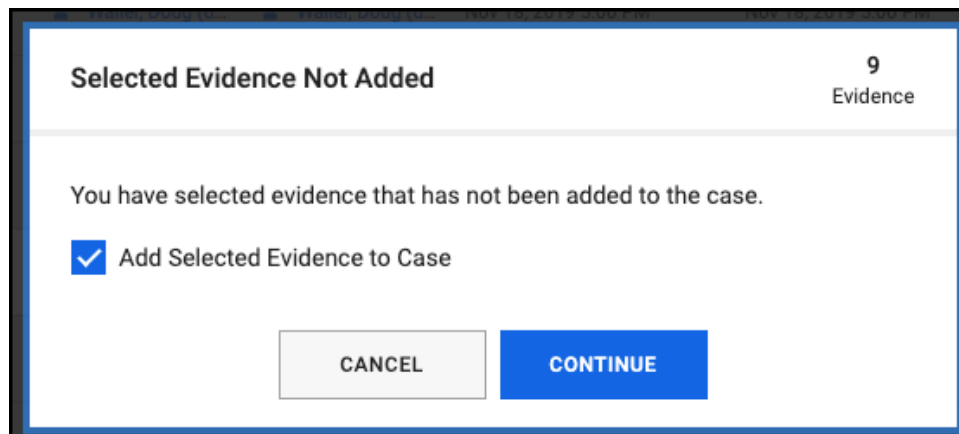
of evidence that was added to the case. You can also review the evidence and remove it from the case.

- **Review** lets you review the evidence files you have selected before adding them to the case. In Review Mode you can view the metadata for the evidence, open the evidence details, or add the evidence to the case.

Adding evidence files is not required to create a case. If you choose not to add any evidence files, you will see a message asking you to confirm that you want to continue creating the case without adding evidence.

5. After adding evidence, click **Review Case Summary**. The Review Case Summary page opens.

If you have selected evidence but not added it to the case before clicking **Review Case Summary**, you will see a message stating that you have selected evidence that has not been added to the case. The “add selected evidence to case” option is selected by default. If you do not want to add the selected evidence to the case, uncheck the box and click **Continue**.



6. On the Review Case Summary page, review the case information to make sure it is correct or to add any additional information.

If you have Edit Case Retention permission, you can set the Retention for the case. The four supported retention policies are:

- **Until Manually Deleted:** This option retains all evidence in cases until manually deleted.
- **Longest Retention Period:** The scheduled deletion date for the case is calculated by finding the longest duration category applied to evidence in the case and adding it to the most recent Recorded On date for any evidence in the case.

- **Specified Date:** Specify a date that sets how long the evidence in the case is retained.
- **Individual Evidence Retention:** The case does not impact retention and each piece of evidence in the case is retained based on its own assigned categories and Recorded On date.

Note: Evidence in multiple cases will use the longest retention policy for the cases.

7. Click **Create Case**. The case will be created, and the Case Details page opens.

For more information about the tabs and actions on the Case Details page, see the [Case Details Page](#).

Searching 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 search pages:

- **All Cases** — Finds all cases, including cases you may not have permission to view. This is the default page for case search.
- **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, no matter what status they are, 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.

Task	Steps
View a case	Click the ID of the case.
Find cases that you own	Click My Cases .
Find cases that are shared with you	Click Shared Cases .
Change search results	<ol style="list-style-type: none"> 1. Update the case search filters. For more information, see Case Search Filters. 2. Click Search.

Task	Steps
Sort search results	Click the column heading for Case ID , Create Date , or Last Update Date . To reverse the sort order, click the heading again.

Working with Case Search Results

On the case search pages — All Cases, My Cases, or Shared Cases — you can take the actions described in this section. To access these actions, click [...] and select an action from the Secondary Actions menu.

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 case owner's First Name and Last Name are in 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.

To export case search results:

1. Search for the cases that you want to export, then click **Export Results**.
2. In the **Select Type** list, select the file format you want to use and 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.

3. If you want to export case search results for additional cases, click **OK** each time the confirmation dialog box appears.

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

Case Search Results Bulk Actions

There are multiple actions you can perform on cases you select from the case search results. To access these actions, click the More Actions menu [...].

Reassign — You can change the owner of a case by reassigning it.

1. Search for the cases that you want to reassign.
2. For each case that you want to reassign, select the check box to the left of the case.
3. Click ... (more actions) and select **Reassign**.

A dialog box appears.

4. In the **Reassign cases** field, start typing the name of the user you want to reassign the case to, wait for Evidence.com to show the list of matching users, then click the name of the user you are looking for.
5. Select the user that you want, then click **Reassign**.
6. In the confirmation dialog box, click **OK**.

The search results will update to show that the user who you selected is now the case owner.

Grant Access — When you need to share a case with users or groups who are in your agency, you can grant access to the case from the results of a case search.

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. Click ... (more actions) and select **Grant Access**.

A dialog box appears.

4. In the **User or Group** field, start typing the name of the user or group you want to share the case with and wait for Evidence.com to show the list of matching users or groups.
5. Select the user or group you are looking for, then click **Share**.

Note: The user or group selected will be granted role based access by default until they are manually removed from the Case Access Control List. To grant the user or group View Only access to the case and related evidence, click the drop-down menu under Access level and select the desired setting. To adjust how long the user or group will

have access to the case and related evidence, click the drop-down menu under Duration and select the desired duration.

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

Update Retention – If you have If you have Edit Case Retention permission, you can set the Retention for the case.

1. Search for the cases whose status you want to update.
2. For each case you want to change the retention of, select the check box to the left of the case.
3. Click ... (more actions) and select **Update Retention**.

Select the retention option for the cases. The four supported retention policies are:

- **Until Manually Deleted:** This option retains all evidence in cases until manually deleted.
- **Longest Retention Period:** The scheduled deletion date for the case is calculated by finding the longest duration category applied to evidence in the case and adding it to the most recent Recorded On date for any evidence in the case.
- **Specified Date:** Specify a date that sets how long the evidence in the case is retained.
- **Individual Evidence Retention:** The case does not impact retention and each piece of evidence in the case is retained based on its own assigned categories and Recorded On date.

Note: Evidence in multiple cases will use the longest retention policy for the cases.

4. Click **Update**.

Update Status — You can change the status assigned to one or more cases in search results.

1. Search for the cases whose status you want to update.
2. For each case you want to change the status of, select the check box to the left of the case.
3. Click ... (more actions) and select **Update Status**.

A dialog box appears.

4. Select the status you want from the drop-down list, then click **Update**.

The search results show the new status you assigned to the cases.

Delete — You can delete cases that are listed in case search results. Cases with a deleted status can still be viewed.

Note: When you delete a case, Evidence.com removes all evidence from the case and 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. Click ... (more actions) and select **Delete**.

A confirmation dialog box appears.

4. Click **Delete**. A notification message box appears.
5. On the notification message box, click **Close**.

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.

View a Case

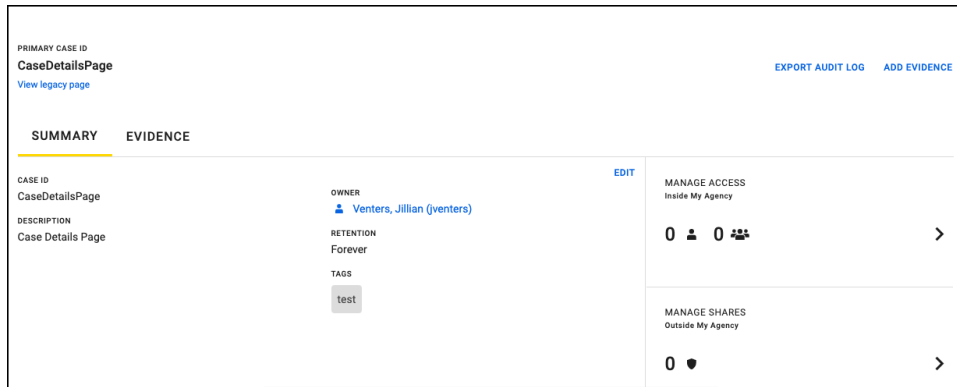
You can view cases listed in the search results if any of the following are true:

- You own the case and your role allows you to view your own case.
- The owner of the case has shared it with you.
- Your user role allows you to view all cases.
- You are an administrator.

To view a case:

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

The Case Details page opens.



Case Details Page

The Case Details page has two tabs:

Summary — This tab shows an overview of information about a case, including the case ID, description, owner, how long the case will be retained, tags, any pinned evidence, and notes. For more information about the actions available on this tab, see [Summary Tab](#).

You can also manage access to the case and share the case to external agencies from the Summary tab. For more information about managing access and shares, see [Cases Access Control Lists](#) and [Sharing Cases to External Agencies](#).

Evidence — This tab shows an overview of information about the evidence attached to the case, including any pinned evidence, evidence folders, and evidence quick views. For more information about the actions available on this tab, see [Evidence Tab](#).

You can export an audit log for a case and add evidence to the case from both the Summary and Evidence tabs on the Case Details page.

Export a Case Audit Log

The audit log of a case shows what updates were made to a case and when, including when tags have been added or removed. You can export a PDF with the entire audit trail, or with information about a specific date range.

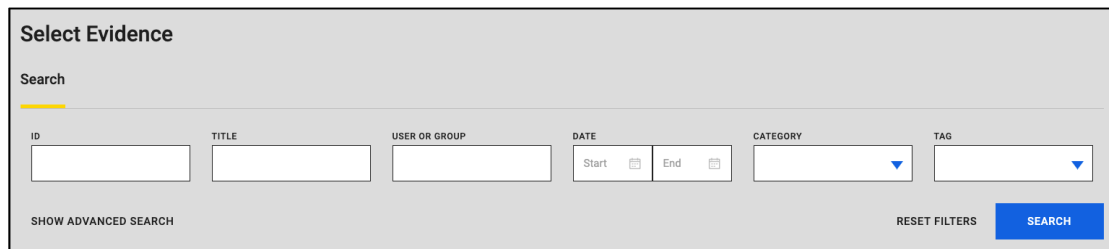
1. On the Case Details page, click **Export Audit Log**.
2. In the Audit Trail dialog box, select the date range you want from the **Date Range** drop-down list.
3. Click **Download**.

The PDF of the export log will open in a separate window. Review the information, then download the PDF.

Add Evidence to a Case

1. On the Case Details page, click **Add Evidence**.

An evidence search page appears.

The screenshot shows a web interface titled "Select Evidence". Below the title is a "Search" label with a yellow underline. The interface contains several search filters: "ID" with a text input field, "TITLE" with a text input field, "USER OR GROUP" with a text input field, "DATE" with "Start" and "End" date pickers, "CATEGORY" with a dropdown menu, and "TAG" with a dropdown menu. At the bottom left is a link "SHOW ADVANCED SEARCH". At the bottom right are two buttons: "RESET FILTERS" and a blue "SEARCH" button.

2. Search for the evidence that you want to add to the case. Use the search filters to refine your results. For more information, see [Case 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.

Note: To upload new evidence to a case, click the **Import** tab on the Evidence Search page.

4. Click **Add to Case** or **Review**.
 - **Add to Case** lets you add the selected evidence to the case without reviewing it.
 - **Review** lets you review the evidence files you have selected before adding them to the case. In Review Mode you can view the metadata for the evidence, open the evidence details, or add the evidence to the case.
5. Click **Done**.

The evidence will now be listed on the Evidence tab of the Case Details page.

If you are adding evidence to a case that has been shared with a partner agency, you will be prompted to update your case share.

Case Evidence Search Filters

Case evidence search filters help you limit search results to the evidence files that you want to see. The displayed search results only include the evidence files that match *all* the search filters that you set.

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

You can also change filter evidence based on certain metadata without changing your entire search using [Case Evidence Search Quick Views](#).

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 Axon Evidence to show the matching groups, and then click the group you want.
- **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.
- **Custom Metadata** — Limits search results to evidence with custom metadata that includes the characters you entered. This field is only available if Custom Metadata is enabled for your agency.

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.

Note: Excluded status was previously used by the Evidence Sync application to exclude evidence from showing up in search results. This status is no longer used by Sync or other Axon applications and is only relevant to evidence uploaded by Sync when it was used.

- **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.
- **Access Class** – Limits search results to evidence access class selected. By default the search results include all access class types.
- **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 Axon Fleet 3, 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.

Case Evidence Search Quick Views

The Case Evidence Search Quick Views lets you filter evidence based on certain metadata without changing your entire search. You can filter evidence based on the following metadata information:

- Evidence that has already been Added or Not Added to the case
- Evidence file type (video, image, and other)
- The user who recorded the evidence

If you click **Reset**, the evidence list will clear your quick view selections and show all the evidence in the original search.

The Quick Views section is automatically updated as evidence is added or removed from a case.

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*.

Import Evidence to a Case

Users who are allowed the Upload External Files permission can import evidence files directly into a case.

The maximum file size is 4 Gigabytes.

1. On the Case Details page, click **Add Evidence**.

An evidence search page appears.

2. Click **Import**.

3. To add files that you want to import, use either of the following methods:

- Find the files on your computer and then drag and drop the files onto the Import Evidence page.

Note: If the Case Subfolder feature is enabled, you can use the Drag and Drop functionality to add a folder and all of its content into the case or case folder. This

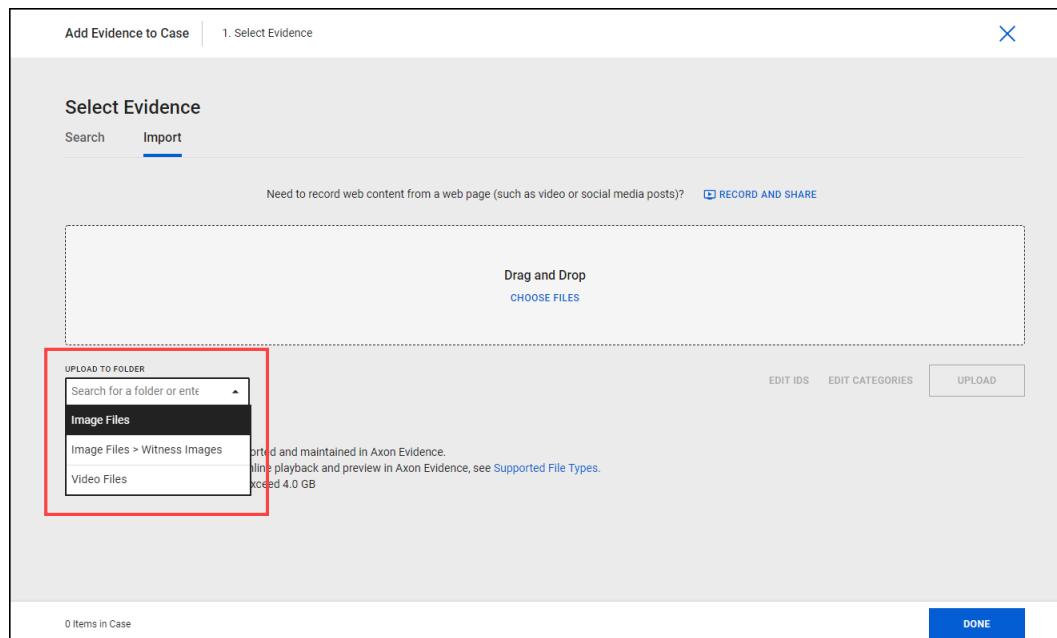
makes it easy to create a folder hierarchy without having to create all the folders before adding evidence.

- Click **Choose Files** and then use the dialog box to find and select the files on your computer.

You can add up to 500 files at one time.

4. Optionally, you can use the **Upload to Folder** list to select the folder or subfolder where the evidence should be uploaded.

Note: This option is only available if the Case Subfolder feature is enabled.



5. Once the files are added, you can edit the Title, ID and Category information individually for each file. You can also edit the IDs and Categories for all the imported evidence or select and edit the IDs and Categories for specific files using the **Edit All IDs** and **Edit All Categories** options.

If your agency has evidence ID field validation enabled, it is enforced when files are uploaded.

Information	Purpose
Title	A meaningful name for the evidence. If you omit the title, Evidence.com assigns the file name as the title.
ID	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 add it to the case.

Information	Purpose
Category	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.

6. Click **Upload**.

The evidence will now be listed on the Evidence tab of the Case Details page.

If you are adding evidence to a case that has been shared with a partner agency, you will be prompted to update your case share.

Summary Tab

The Summary tab on the Case Details page shows an overview of information about a case including the case ID, description, owner, how long the case will be retained, tags, any pinned evidence, and notes.

Edit the Case ID, Description, Owner, or Retention of a Case

1. On the Case Detail page Summary tab, click **Edit**.
2. Enter your changes.

The screenshot displays the 'Summary' tab of a case details page. At the top, there's a navigation bar with tabs: EVIDENCE, RESPOND, CASES (highlighted), INVENTORY, REPORTS, ADMIN, and HELP. Below this, a header bar shows '← BACK TO CASES' and 'Last updated: Dec 7, 2020 3:37 PM by Schuer, David (10-101)'. The main content area has a 'PRIMARY CASE ID' of 'UID-201126-025' and a 'SUMMARY' tab selected. The 'EVIDENCE (5)' tab is also visible. The 'CASE ID' field contains 'UID-201126-025'. The 'DESCRIPTION' field contains 'Home robbery'. The 'OWNER' field shows 'Schuer, David (10-101)' with a dropdown arrow. The 'RETENTION' field shows 'Until Manually Deleted' with a dropdown arrow. There are 'CANCEL' and 'SAVE' buttons. On the right, there are sections for 'MANAGE ACCESS' (Inside My Agency) and 'MANAGE SHARES' (Outside My Agency), both showing 0 items. There are also 'EXPORT AUDIT LOG' and 'ADD EVIDENCE' buttons.

- If you are changing the owner of the case, start typing the name of the user in the **Owner** field that you want to reassign the case to, wait for Evidence.com to show the list of matching users, then click the name of the user you are looking for.
- If you have Edit Case Retention permission, you can set the Retention for the case. Select the retention option for the cases. The four supported retention policies are:

- **Until Manually Deleted:** This option retains all evidence in cases until manually deleted.
- **Longest Retention Period:** The scheduled deletion date for the case is calculated by finding the longest duration category applied to evidence in the case and adding it to the most recent Recorded On date for any evidence in the case.
- **Specified Date:** Specify a date that sets how long the evidence in the case is retained.
- **Individual Evidence Retention:** The case does not impact retention and each piece of evidence in the case is retained based on its own assigned categories and Recorded On date.

Note: Evidence in multiple cases will use the longest retention policy for the cases.

3. Click **Save**.

Add and Remove Tags for a Case

Tags are labels that you can apply to cases and evidence. You can use tags to filter search results to find a case or evidence more easily.

Tags are located on the Summary tab of the Case Details 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".



The following table shows the steps for tag-related tasks:

Action	Steps
Add a tag	<ol style="list-style-type: none"> 1. Click Edit on the Summary tab of a Case Details page. 2. In the Tags field, start typing a tag name. 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. If the tag doesn't already exist, add the new tag name, then click Add Tag. 5. Click Save. Evidence.com adds the tag to the case.

Action	Steps
Remove a tag	<ol style="list-style-type: none">1. Under Tags, find the tag that you want to remove and click X.2. Click Save. Evidence.com removes the tag from the case.

Case Notes

The Notes section of the Summary tab organizes comments on the case from users, with the newest notes at the top of the section.

To add a note to a case:

- Type in the **New Note** field, then click **Add Note**.

To edit or delete an existing note on a case:

1. Hover your mouse pointer over an existing note.
2. Click the Secondary Actions menu button [...] and select **Edit** or **Delete**.
 - **Edit:** Make your changes and click **Save Note**. When you edit a note, the note is updated to list you as the author of the note.
 - **Delete:** Click **Delete** in the confirmation window.

Evidence Tab

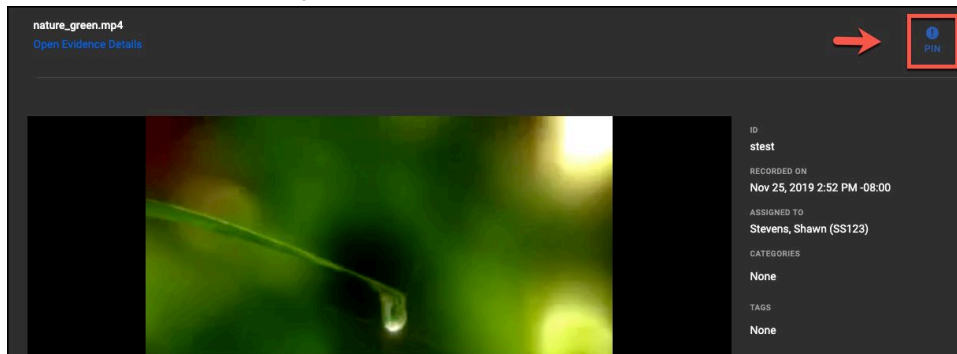
This tab shows an overview of information about the evidence attached to the case, including any pinned evidence, evidence folders, and evidence quick views.


Pin Evidence

Pinning evidence is a way to keep the most relevant or critical evidence at the top of the evidence and summary sections in a case. Evidence can only be pinned in a case when you are reviewing it.

1. On the Evidence tab, select the check box of the evidence you want to pin to the case, then click **Review**.

2. After the evidence file opens in Review Mode, click **Pin**.



3. Click  to return to the Evidence tab.

Note: If you click **Review All**, you can pin each piece of evidence as you review it.

Evidence Quick Views

The Evidence Quick Views let you quickly navigate evidence based on the following metadata information:

- Evidence file type.
- The user who recorded the evidence.
- The evidence ID.

For example, if the File Type section shows there are images, videos, and audio recordings files, you can select Image, and the evidence list will show only image file types. If you click **Reset**, the evidence list will clear your selections and show all the evidence in a case.

In situations where there are more than five items associated with any metadata type (File Type, Recorded By, or ID), the list is condensed and only the first five items are shown along with text saying how many More items are in the list. Clicking the **More** option expands the list to show all the items and provides a **Show Less** option to condense the list.

The Quick Views section is automatically updated as evidence is added or removed from a case.

Case Evidence Filters

Case evidence filters help you search for specific evidence attached to a case based on the metadata of the evidence. You can select multiple filters to use for searching, but the results will only include evidence contained in the case that match all of the filters you use.

Each filter will only contain values that exist on the evidence in the case. For example, the category filter will only display categories that exist on evidence in the case. These dropdown

menus on the filters allow you to select multiple values from the dropdown menu. When multiple values are selected the system does an OR search, so evidence matching any of the selected values will be returned.

You can click **Reset** in the Filters list to clear your selections and show all the evidence in a case.

- **ID** — Filters the list of evidence by ID. For more information, see [Text Search Details](#).
- **Title** — Filters the list of evidence by matching titles.
- **Recorded By** — Filters the list of evidence by the user who recorded the files.
- **Uploaded By** — Filters the list of evidence by the user who uploaded the files.
- **On Access List** — Filters the list of evidence by the users or groups who have access to the files.
- **Recorded On** — Filters the list of evidence by the date the files were recorded.
- **Uploaded On** — Filters the list of evidence by the date the files were uploaded.
- **Deleted On** — Filters the list of evidence by the date the files were deleted.
- **Category** — Filters the list of evidence by the category you select. By default, the search results include evidence assigned to any category, including uncategorized cases.
- **Tag** — Filters the list of evidence by the selected tags. For more information, see [Text Search Details](#).
- **File Type** — Filters the list of evidence by the selected file types.
- **Status** — Filters the list of evidence by the selected status. For example, selecting *Pending Triage* would only show evidence files with that status. By default, case searches include all statuses.
- **Source** — Filters the list of evidence by evidence source. For example, selecting *Body Worn Cameras* would only show evidence files recorded by that hardware.
- **Restricted** — Filters the list of evidence to only files that are restricted. By default, the restriction filter is not enabled.
- **Device** — Filters the list of evidence by device serial number.

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, the search results will include any evidence with 21 in any portion of the ID, such as *2197* and *446219*.
- 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 *172182*.

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

Remove Evidence from a Case

You can remove evidence from a case from the Evidence tab of the Case Details page.

1. On the Evidence tab, select the ID of the evidence you want to remove.
2. Click the Secondary Actions menu button [...] and select **Remove from case**.
3. In the confirmation message box, click **Remove**.

When the evidence is removed from the case, it is returned to its normal retention schedule based on the category assigned to the evidence and the date the evidence was recorded on.

Working with Evidence Folders

Evidence folders provide a way to organize evidence files. After you add evidence to a case, you can create as many folders as you need, rename folders, and add evidence to multiple folders. Evidence added to folders will also be shown in the All Evidence list.

Add a Folder to a Case

1. On the Evidence tab of the Case Details page click **Create a Folder**. The Create a Folder dialog is shown.
2. Enter a meaningful name for the folder in the **Folder Name** field, then click **Create**.

Axon Evidence creates the folder and adds it to the folder list. If any evidence files were selected when you create the folder, that evidence will be automatically added to the folder when it is created.

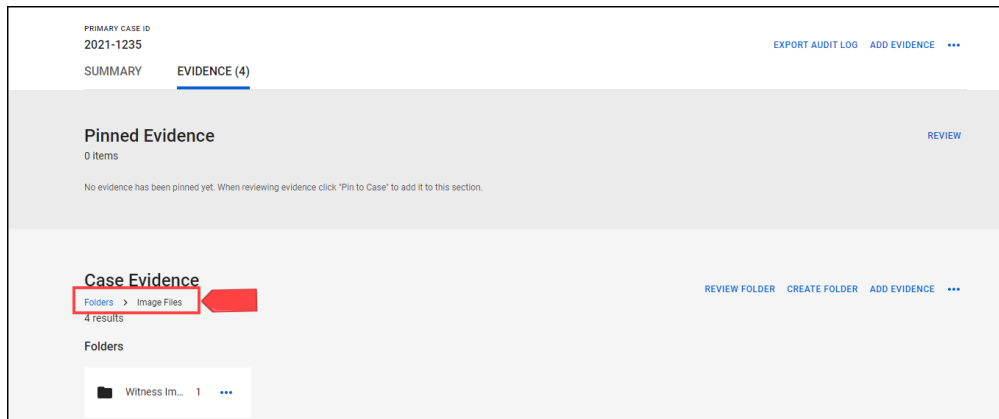
Add a Case Subfolder

Note: The Case Subfolder feature currently is not enabled by default. If you choose to enable this feature, it cannot be disabled in the future due to changes in the data structure. If your agency would like to use this feature, contact your Axon representative.

When you are inside a case folder you can add a case subfolder to the folder.

1. On the Evidence tab of the Case Details page, click on the folder where you want to add the subfolder.

The folder trail is shown under the Case Evidence title. In the example image below, the user is in the Image Files folder of the case.



2. Click **Create a Folder**. The Create a Folder dialog is shown.
3. Enter a meaningful name for the subfolder folder in the **Folder Name** field, then click **Create**.

The subfolder is added to the case.

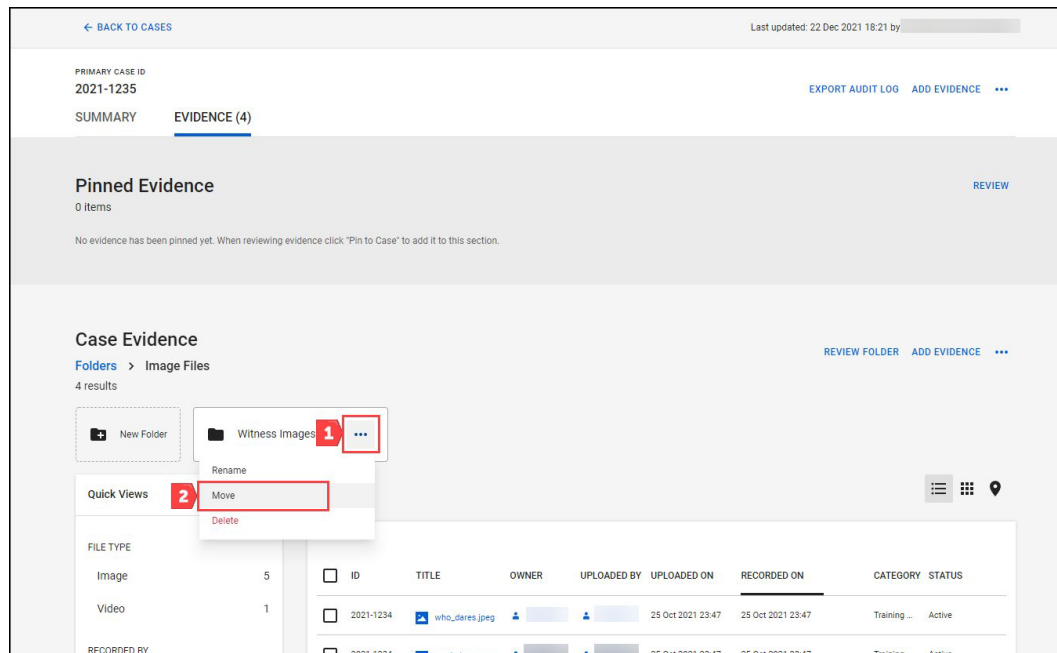
Move a Case Subfolder

Note: The Case Subfolder feature currently is not enabled by default. If you choose to enable this feature, it cannot be disabled in the future due to changes in the data structure. If your agency would like to use this feature, contact your Axon representative.

You can move a case subfolder to different locations within the case folder.

1. On the Evidence tab of the Case Details page, click on the case folder where the subfolder you want to move is located.

- Click the **More Actions** icon on the subfolder you want to move and select **Move**.



- Axon Evidence asks you to select a destination folder. Then click **Move Here** to move the subfolder.

Note: Subfolder names cannot be duplicated within a folder. If the selected destination folder already has a subfolder with the same name as subfolder you want to move, you are asked if you want to cancel the move so you can rename one of the subfolders or merge the contents of the subfolders.

The 'Move To Folder' dialog box is shown. It has a title bar with a close button (X). Below the title bar is a section labeled 'FOLDER NAME' with a search input field containing the text 'Search for a folder or enter new folder name'. At the bottom, there is a list showing '1 folder'. To the right of the list are two buttons: 'CANCEL' and 'MOVE HERE'.

Rename a Folder

- On the Evidence tab of the Case Details page, click the name of a folder or subfolder.
- Click the Secondary Actions menu [...] and select **Rename Folder**.
- Type the new name in the **Name** box, then click **Rename**.

Add Evidence to a Folder

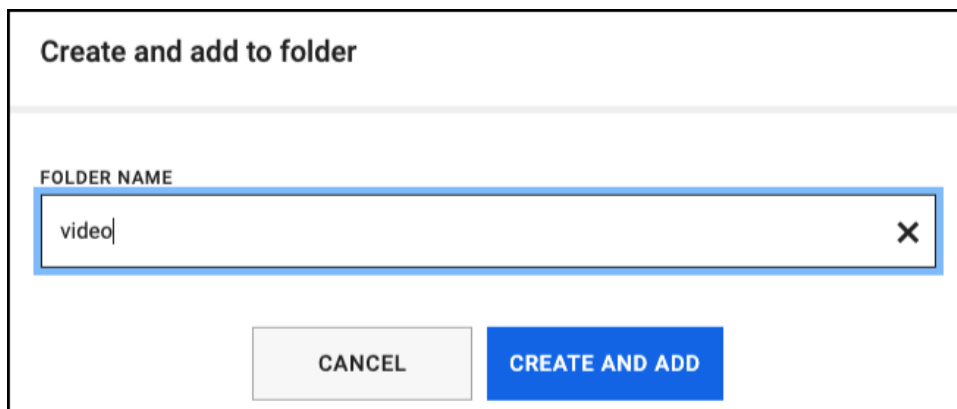
You can add the evidence that is already part of a case to any evidence folder that you need.

For information about adding evidence to a case, see [Add Evidence to a Case](#).

1. In the All Evidence section of the Evidence tab, select the check box to the left of the evidence ID of each file you want to add to a folder.
2. Above the evidence list, click **Add to Folder**.
3. In the dialog box, in the **Select Folder** list, select the folder or subfolder that you want to add the evidence to, then click **Add**.

If the folder you want to add evidence to does not exist, begin typing a folder name and a new row will appear in the dialog box with (new) in parenthesis after the name. Select the folder.

Selecting this option will change the workflow from adding evidence to a folder to creating a new folder and adding evidence to that new folder. When you click **Create and Add**, the previously selected evidence will be added to the newly created folder.



The screenshot shows a dialog box titled "Create and add to folder". Inside the dialog, there is a text input field with the label "FOLDER NAME" above it. The input field contains the text "video". To the right of the input field is a small square button with an "X" icon. Below the input field, there are two buttons: a light gray button labeled "CANCEL" and a blue button labeled "CREATE AND ADD".

4. If you want to confirm the evidence is in the folder you added it to, click the folder name and view the evidence list.

Importing Evidence into a Folder

You can import evidence directly into a case folder or subfolder.

Note: This option is only available if the Case Subfolder feature is enabled.

Users who are allowed the Upload External Files permission can import evidence files directly into a case.

The maximum file size is 4 Gigabytes.

1. On the Case Details page, click **Add Evidence**.

An evidence search page appears.

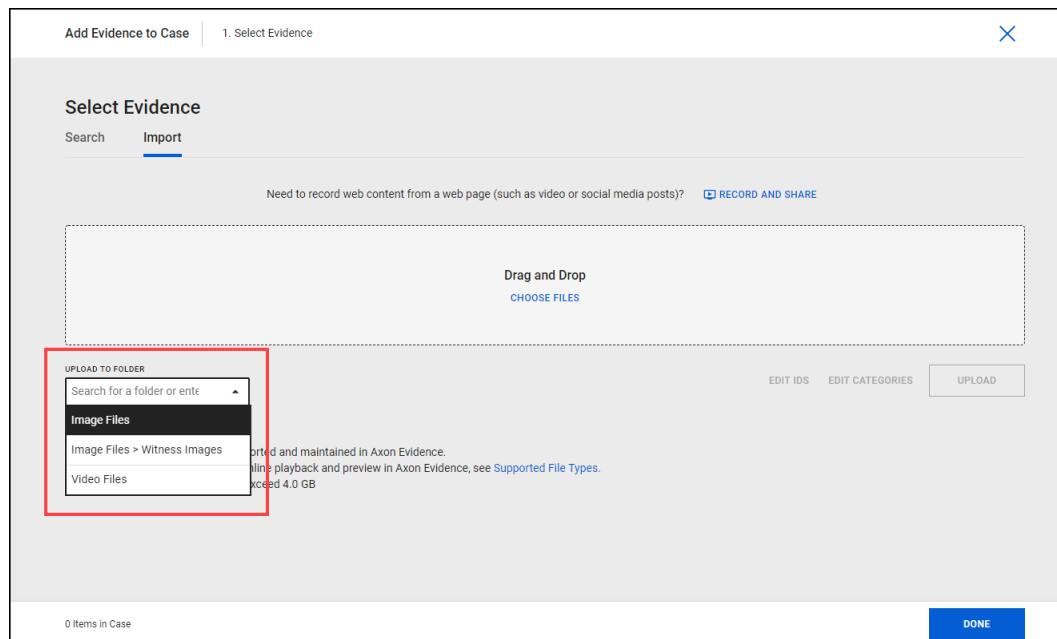
2. Click the **Import** tab.

3. To add files that you want to import, use either of the following methods:

- Find the files on your computer and then drag and drop the files onto the Import Evidence page.
- Click **Choose Files** and then use the dialog box to find and select the files on your computer.

You can add up to 500 files at one time.

4. Optionally, you can use the **Upload to Folder** list to select the folder or subfolder where the evidence should be uploaded.



5. Once the files are added, you can edit the Title, ID and Category information individually for each file. You can also edit the IDs and Categories for all the imported evidence or select and edit the IDs and Categories for specific files using the **Edit All IDs** and **Edit All Categories** options.

If your agency has evidence ID field validation enabled, it is enforced when files are uploaded.

Information	Purpose
Title	A meaningful name for the evidence. If you omit the title, Evidence.com assigns the file name as the title.
ID	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 add it to the case.
Category	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.

6. Click **Upload**.

The evidence will now be listed on the Evidence tab of the Case Details page.

If you are adding evidence to a case that has been shared with a partner agency, you will be prompted to update your case share.

Remove Evidence from a Folder

You can remove evidence from any evidence folder as needed.

If you need to remove evidence from a case, see [Remove Evidence from a Case](#).

1. On the Evidence tab, click the folder that you want to remove evidence from.

Below the evidence preview area, a list of evidence in the folder appears.

2. Select the check box for each piece of evidence that you want to remove from the folder.
3. Click the Secondary Actions menu button [...] and select **Remove from Folder**.
4. In the confirmation message box, click **Remove**.
5. In the message box, click **OK**.

Evidence.com removes the selected evidence from the folder. The evidence remains in the case in the All Evidence section.

Working with Evidence in a Case

For evidence that is in a case, you can perform the actions described in this section. To learn more about working with evidence, see the [Evidence section on the Axon Help Center](#).

Review Evidence in a Case

You can review evidence in a case on the Evidence tab. While all evidence file types can be added to Review mode, only file types that are currently supported by Evidence.com will be displayed. If the file type is unsupported, you will be prompted to download the evidence.

1. In the evidence list on the Evidence tab, select the check box of the evidence you want to review.
2. Click **Review**.

Note: If you click **Review All** without selecting any evidence, all the evidence on the page will open in Review mode.

Evidence Bulk Actions

The bulk actions menu provides ways to categorize or organize multiple pieces of evidence. The bulk actions you can perform are the following:

- Update the metadata of evidence files.
 - **Update ID**
 - **Add Category**
 - **Update Evidence Group**
 - **Reassign**
- Manage the access to evidence.
 - **Inside my agency** — This action allows you to change the access levels, duration, and users for the selected evidence files.
 - **Outside my agency** — This action has two options:
 - Add Name to External Access List:** Send people outside your agency a link to the selected piece of evidence, and give them permissions to download, view the audit trail, and post notes for selected pieces of evidence. You can also set how long the link to the evidence will be active and give permission for the people to reshare the evidence.
 - Email a Download Link:** Send people outside your agency a link to the selected piece of evidence and set the permissions for including audit trails and a table of contents. You can also set how long the link to the evidence will be active.

- **Restrict** — This action allows you to restrict access to the evidence to users and groups on the access control list and users in roles with the view restricted evidence permission.
- Take additional actions on evidence files.
 - **Auto-Transcribe** – This action applies to audio and video files. If you have permission to request an Auto-Transcript, you can bulk request transcriptions. See [Bulk Requests from the Case Details Evidence Tab](#) for more information.
 - **Redact** — This action only applies to video files. It will apply a full-screen blur filter to the video and create the blurred file as a child piece of evidence to the original.
 - **Download** — This allows you to download the selected evidence.
 - **Export List** — This allows you to export a list that contains information about the evidence, including ID, evidence group, owner, when the evidence was recorded, who uploaded the evidence, and the status.
 - **Remove from case**
- Manage evidence folders.
 - **Rename Folder**
 - **Delete Folder**
 - **Remove from Folder**

To use any of the bulk actions:

1. Select multiple pieces of evidence by selecting the check box to the left of the evidence ID.
2. Click the Secondary Actions menu button [...] in the left corner of the All Evidence section, then select an action from the drop-down list.

Download Evidence from a Case

You can download evidence included in a case from the Case Details page.

1. On the Evidence tab of the Case Details page, select the check box of the evidence files you want to download.
2. Click the Secondary Actions menu button [...] and select **Download**.

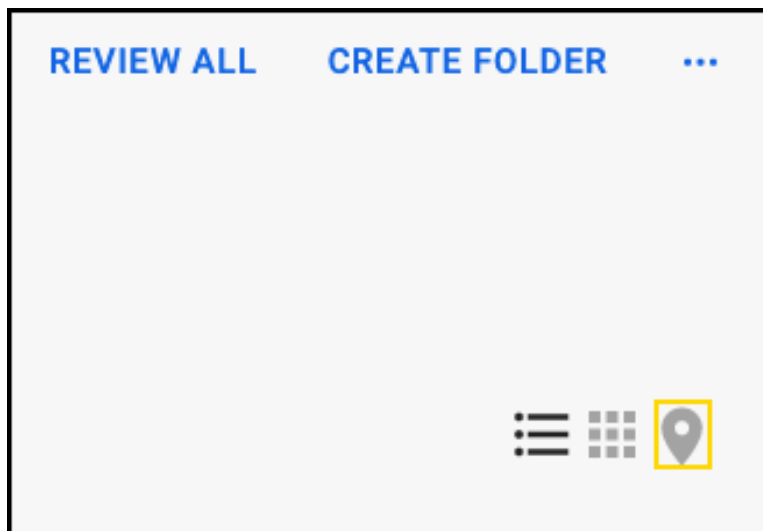
3. In the Configure your bulk download screen, select the download format and if you want to include the Audit Trail and Table of Contents in the download file, then click **Download**.

The evidence files will be bundled into a file, and an email containing a download link will be sent your email address.

View a Case Map

If evidence in a case has location information, you can view the evidence in an evidence map.

- On the Evidence tab of the Case Details page, in the All Evidence section, click the map icon.



Case Evidence Map Actions

The case evidence map provides 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.

Action	Steps
See information about evidence	<ol style="list-style-type: none"> 1. Click on the icon for the evidence. Evidence.com shows information about the evidence. 2. If you want to see more information about the evidence, click View Evidence. The Evidence Detail page opens.

Action	Steps
Pan	<ol style="list-style-type: none"> 1. Position the mouse pointer over the map. 2. Click and hold the mouse button. 3. Move the mouse to pan the map. 4. Optionally, click Redo Search in this Area to see additional evidence in the new map view.
Zoom In or Zoom Out	<ul style="list-style-type: none"> • In the map, click on the + or – icons to zoom in or out. <p>Alternately, if your mouse has a mouse wheel:</p> <ol style="list-style-type: none"> 1. Position the mouse pointer over the map. 2. Rotate the mouse wheel to zoom in or out. <p>If needed, click Redo Search in this Area to see additional evidence in the new map view.</p>

Case Access Control Overview

Axon Evidence's cases functionality utilize access classes to control access to cases. Each case in Axon Evidence is assigned to one of the following access classes:

- Unrestricted
- Restricted
- Confidential

Cases can only be assigned to one access class at a time. By default, cases are created in Axon Evidence with the Unrestricted access class. However, users with the appropriate permissions can set the case's access class either during or after the case creation workflow.

When a case access class is changed to restricted or confidential, all evidence in the case will inherit the case's access class

Note: There are no Axon Evidence specific definitions for the Restricted and Confidential access classes. Your organization should determine how these classes are used within your organization.

User Access to Case and User Permissions

Default access to case is based on the permissions for a user's assigned role. The role-based permissions affect a user's ability to search for, view, and change the access class for cases.

Additionally, each case has its own access list, which allows your organization to manage case access inside your agency on an as needed basis. Users and groups inside your

organization can be granted access to a case by being added to the case access list. Users and groups on the case access list are able to view the case and all evidence in the case.

The following table provides information on a user's ability to search for, view, and change the access class for a case for the different permission settings.

Permission	Setting	Role-Based Access		Access List Member
		User	Group Monitor	
List Unrestricted Cases List Restricted Cases List Confidential Cases	Prohibited	No Cases	NA	Can search and run reports if on the case access list
Sets permission to search for cases, review audit trails, and include case in reports case for the set access class.	Only Their Own	If assigned as case owner	NA	Can search and run reports if on the case access list
	Any case	Any Case	NA	Can search and run reports if on the case access list
View Unrestricted case View Restricted case View Confidential case	Prohibited	No case	NA	Can view case if on the access list
Sets permission to access case for the set access class	Only Their Own	If assigned as case owner	NA	Can view case if on the access list
	Any case	Any case	NA	Can view case if on the access list
Apply Access Class -Restricted Apply Access Class – Confidential	Prohibited	Cannot apply access class	NA	No effect
Sets permission to apply the access class	Only Their Own	If assigned as case owner	NA	No effect
	Any case	Any case	NA	No effect
Remove Access Class – Restricted Remove Access Class – Confidential	Prohibited	Cannot remove access class	NA	No effect
Sets permission to remove the access class	Only Their Own	If assigned as case owner	NA	No effect
	Any case	Any case	NA	No effect

Case Search Page Views

The information shown to users on the Case Search page and in reports depends on the permissions for the user's assigned role and if the user has been added to a case access list. Users are only allowed to search for cases that their role grants them permission to list and that they are on the access list for. If a user's role does not include permission to list a case

and the user is not on the access list for the case, then the user will not be able to search for the case and the case will not appear in any reports.

Example: If a user's assigned role has the List Unrestricted case permission set to Only Their Own and the user is not on any case access lists, then the user will not see any cases that they are not the case owner of, Restricted Cases, or Confidential Cases on the Case Search page.

If a user has list permission for an access class set to Only Their Own, then the user will only see the cases they are assigned as the owner.

Note: This user would not see other users "Unrestricted" Cases and the "Owner" search filter is locked with the current user's name that is signed into Axon Evidence

CASE ID: OWNER: MAC, GMAC (8675309) CREATED ON: Start End UPDATED ON: Start End STATUS: TAG:

SHOW ADVANCED SEARCH RESET FILTERS [SEARCH](#)

Cases [CREATE CASE](#) [EXPORT RESULTS](#) [...](#)

3 results

<input type="checkbox"/>	CASE ID	OWNER	CREATED ON	LAST UPDATED ON	STATUS
<input type="checkbox"/>	nicks case3	MAC, GMAC (8675309)	Feb 22, 2021 6:18 PM	Mar 23, 2021 9:16 PM	Active
<input type="checkbox"/>	nic and gav	MAC, GMAC (8675309)	Mar 3, 2021 11:52 AM	Mar 19, 2021 2:10 PM	Active
<input type="checkbox"/>	sharing evidence	MAC, GMAC (8675309)	Feb 18, 2021 10:06 PM	Mar 19, 2021 2:05 PM	Deleted

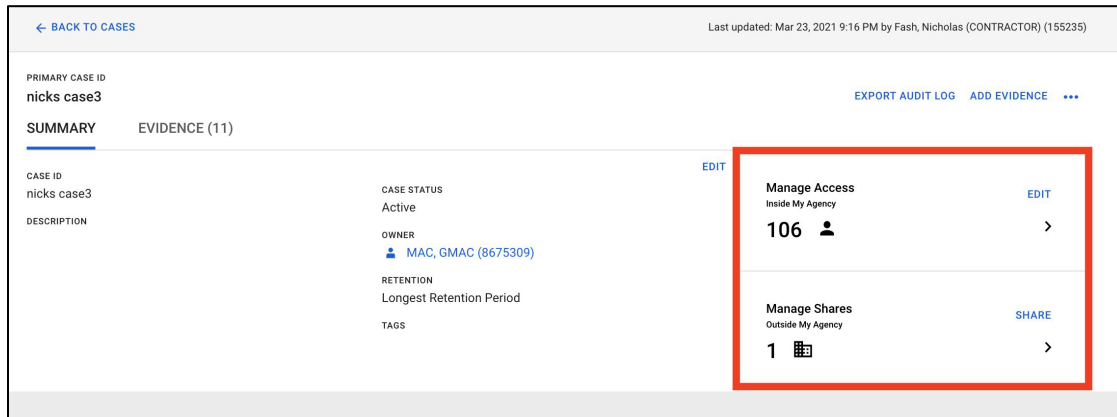
< 1 >

3 Results

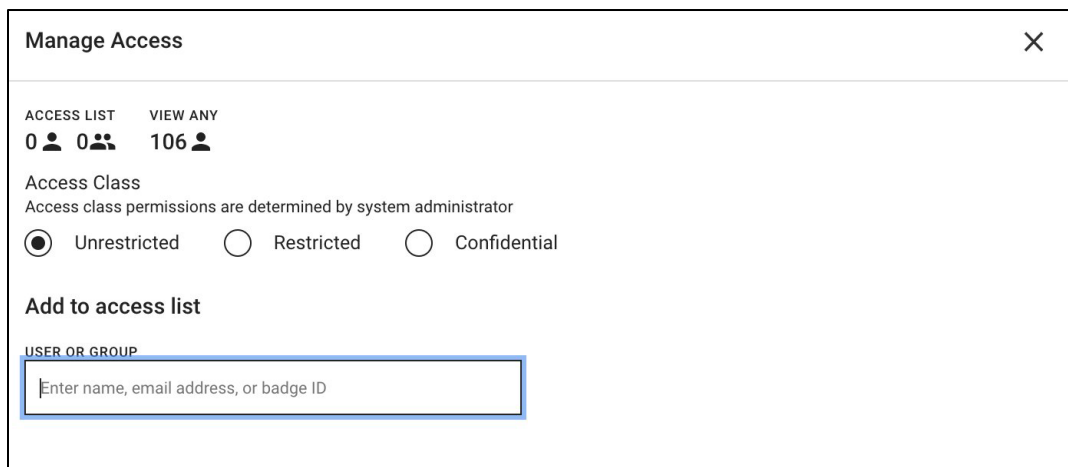
Access List Information

You can get a snapshot view of the number of users that can access a case by looking at the manage access section of the Case Details page. The following image shows that 106 users

inside your organization have access to the case and that it has been shared with 1 agency outside your organization.



A detailed view of user access can be found by clicking **Manage Access** to view the Manage Access screen for the case. The upper portion of the Manage Access screen shows the number of users and groups on the access list, the number of users that can view the case due to their role-based permissions, and the access class for the case.



The Manage Access screen is also used to add and remove users and groups from the case access list and to change the case access class. Users must have the appropriate permission to apply or remove an access class. Since applying either the restricted or confidential access class to a case will apply the same access class to all evidence in the case, the user must have both permission to set the access class on the case and all evidence in the case. The lower portion of the Manage Access screen shows the users and groups on the access list for the case. The list shows the user or group name, access level, case access duration, and when the user or group was added to the list. If the case is in the restricted or confidential access class, then only users in roles that grant them access to cases in the restricted or confidential access class and the users and groups on the access list can view the case.

Evidence Access vs Case Access

Axon Evidence provides administrators flexibility in which permissions they grant to their users. As such, it is possible to configure roles in such a way that a user may be able to access a case, but not be able to access all evidence in the case. For example, a user role could include permission to list and view all restricted cases, but not include permission to list and view restricted evidence. In this scenario, the user would be able to search for and view the case, however they would only be able to list and view the evidence in the case that either their role grants them default access to or that they are on the access control list for.

You can ensure that a user has access to both a case and all evidence in the case by adding the user to the case access control list.

Changing Case Access Class

After a case is created, the access class for the case can **only** be changed by navigating to the **Manage Access** page inside a case and manually changing the case access class.

Changing the access class of a case only allows users that are on the case access list or that have list and view permissions for the access class to search for and view the case. Users that do not have list permission cannot see the case on the case Search page.

Changing case Access Class from the case Detail Page

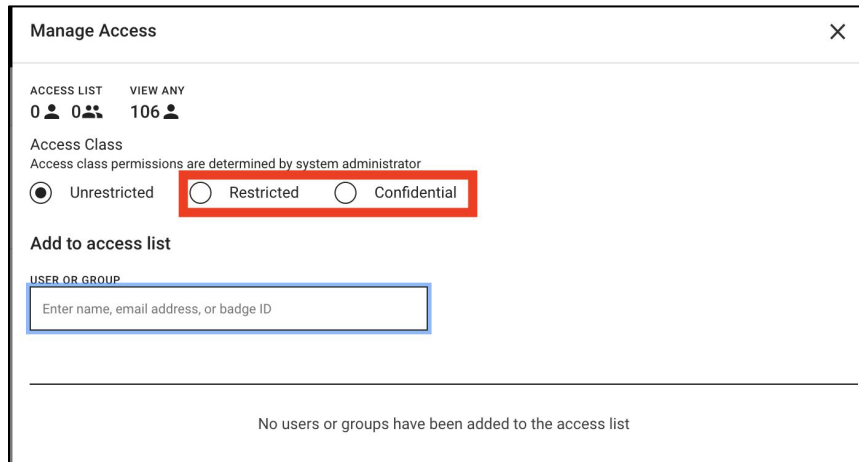
From the Manage Access section you can add users and groups to the access list for a case file and change the case's access class.

1. On the case Detail page click **Manage Access**.

The screenshot displays the Axon Evidence interface for a case detail page. At the top, there is a navigation bar with a '← BACK TO CASES' link on the left and a 'Last updated: Mar 23, 2021 9:16 PM by Fash, Nicholas (CONTRACTOR) (155235)' timestamp on the right. Below the navigation bar, the page is divided into two main sections. The left section contains case metadata: 'PRIMARY CASE ID' (nicks case3), 'SUMMARY' (selected), 'EVIDENCE (11)', 'CASE ID' (nicks case3), and 'DESCRIPTION'. The right section contains case details: 'CASE STATUS' (Active), 'OWNER' (MAC, GMAC (8675309)), 'RETENTION' (Longest Retention Period), and 'TAGS'. On the far right, there is a 'Manage Access' section, which is highlighted with a red box. This section shows '106' users and an 'EDIT' link. Below it, there is a 'Manage Shares' section showing '1' share and a 'SHARE' link.

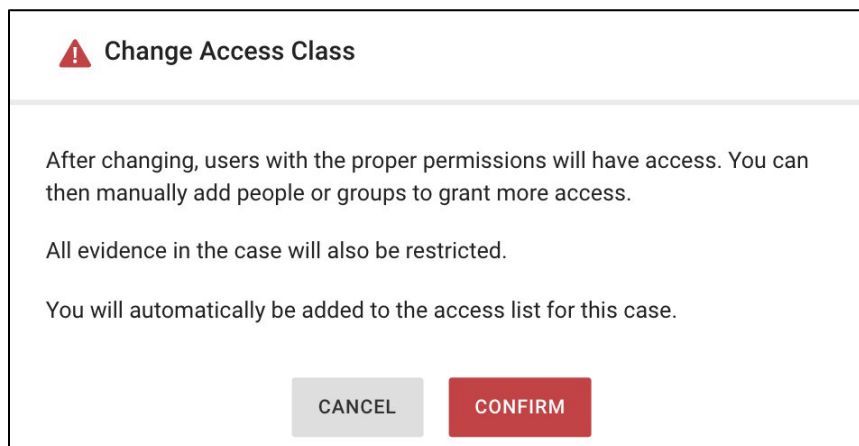
The Manage Access screen is shown on the right side of the page.

2. In the Access Class, select **Restricted** or **Confidential**.



The 'Manage Access' dialog box has a title bar with a close button (X). It contains two tabs: 'ACCESS LIST' and 'VIEW ANY'. Under 'ACCESS LIST', there are icons for 0 users and 0 groups. Under 'VIEW ANY', there are icons for 106 users. The 'Access Class' section has a note: 'Access class permissions are determined by system administrator'. Below this are three radio buttons: 'Unrestricted' (selected), 'Restricted', and 'Confidential'. The 'Restricted' and 'Confidential' buttons are highlighted with a red rectangle. Below the radio buttons is a section titled 'Add to access list' with a sub-label 'USER OR GROUP'. It contains a text input field with the placeholder 'Enter name, email address, or badge ID'. At the bottom, a message states 'No users or groups have been added to the access list'.

The system asks you to confirm that you want to restrict the case. Since the access class applied to the case will also be applied to all evidence in the case, the user will only be allowed to apply the selected access class to the case if they have permission to apply the access class to the case and all evidence in the case.



The 'Change Access Class' dialog box features a red warning triangle icon and the title 'Change Access Class'. The main text reads: 'After changing, users with the proper permissions will have access. You can then manually add people or groups to grant more access.' Below this, it states: 'All evidence in the case will also be restricted.' and 'You will automatically be added to the access list for this case.' At the bottom, there are two buttons: a grey 'CANCEL' button and a red 'CONFIRM' button.

Click **Confirm** 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 case informing them that the case access class was updated, but that they still have access.

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

Manage Access

ACCESS LIST VIEW ANY
1 0 106 Restricted

Access Class
Access class permissions are determined by system administrator
☐ Unrestricted ☒ Restricted ☐ Confidential

Add to access list

USER OR GROUP
Enter name, email address, or badge ID

NAME	MEMBERS	ACCESS TYPE	DURATION	ADDED ON
MAC, GMAC (8675309)		Manual	Until Removed	Mar 25, 2021

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 case and the evidence in the case depends on the permissions associated with their assigned role.
 - If **View** is selected, the user can only view the case and the evidence in the case.

Manage Access

ACCESS LIST VIEW ANY
0 0 106

Access Class
Access class permissions are determined by system administrator
☒ Unrestricted ☐ Restricted ☐ Confidential

Add to access list

USER OR GROUP
Enter name, email address, or badge ID

ACCESS L...
Role

DURATION
Until Removed

183375 Holland Noah x

5783872 Matthew Carlson x

ADD

5. From the **Duration** list, select the period of time the user can access the case.

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

Manage Access

ACCESS LIST: 1 user, 0 groups. VIEW ANY: Restricted

Access Class: Access class permissions are determined by system administrator.
☐ Unrestricted ☒ Restricted ☐ Confidential

Add to access list

USER OR GROUP: Enter name, email address, or badge ID

ACCESS L...: Role

DURATION: Until Removed

5783872 Matthew Carlson x

183375 Holland Noah x

ADD

NAME	MEMBERS	ACCESS TYPE	DURATION	ADDED ON
MAC, GMAC (8675309)		Manual	Until Removed	Mar 25, 2021

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 case.

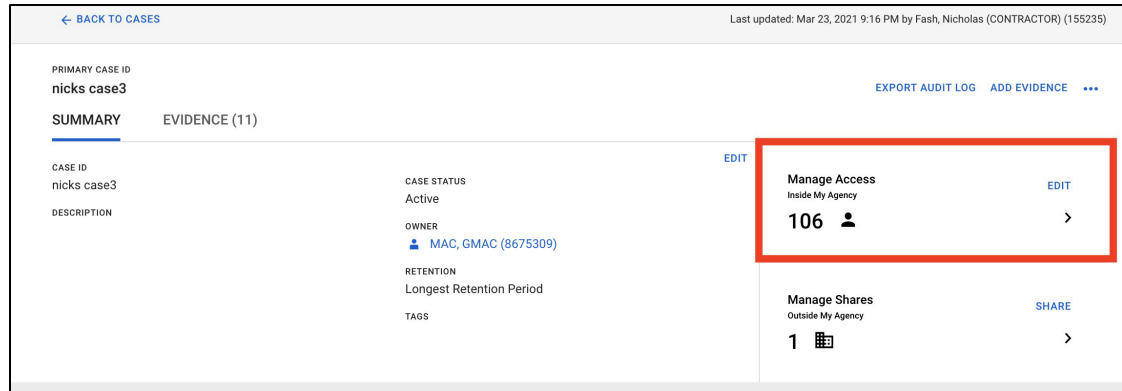
7. Repeat steps 3 through 6 to add other users.

8. After all users and groups are added, click **Done** to return to the Case Detail page.

Removing a Restricted or Confidential Access Class from a Case

The Restricted and Confidential access classes can only be removed from the case Detail page.

1. On the case Detail page click **Manage Access**.



The Manage Access screen is shown on the right side of the page.

2. In the Access Class, select **Unrestricted**.
3. Click **Done** to return to the case Detail page.

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

Note: Evidence will inherit the case access class if changed to **Restricted** or **Confidential**. If a user changes the Case Access Class to **Unrestricted**, the evidence within the case will **not** inherit the **Unrestricted Access Class** and will remain **Restricted** or **Confidential**

Granting Case Access

Users and Groups inside your agency can be granted access to cases from both the Case Search and Case Detail pages. However, Case Access lists can only be modified from the Case Details Page.

Adding Users and Groups to an Inside My Agency Access List from the Case Search Page

From the case search page, you can add users and groups to the access list for multiple cases at the same time.

Note: This procedure can also be used to add users and groups to the access list for case with a Restricted or Confidential access class.

1. Search for the cases you want to grant access to.
2. In the search results, select the check box to the left of the Case ID for each case file that you want to grant access to.

3. Click the ... (more actions) menu and select **Grant Access**.

The screenshot displays the 'Cases' management interface. At the top, there are tabs for 'ALL CASES', 'MY CASES', and 'SHARED CASES'. Below these are search filters for 'CASE ID', 'OWNER', 'CREATED ON', 'UPDATED ON', 'STATUS', and 'TAG'. A 'SHOW ADVANCED SEARCH' link and a 'RESET FILTERS' button are also present. The main section is titled 'Cases' and shows '397,298 results | 1 selected'. A table lists cases with columns for 'CASE ID', 'OWNER', 'CREATED ON', and 'LAST UPDATED ON'. The first case, 'nicks case3', is selected. To the right of the table, a 'more actions' menu is open, showing options like 'Reassign', 'Grant access' (highlighted with a red box), 'Update retention', 'Update status', 'Delete', and 'OTHER ACTIONS' (including 'Create case' and 'Export results').

CASE ID	OWNER	CREATED ON	LAST UPDATED ON
<input checked="" type="checkbox"/> nicks case3	MAC, GMAC (8675309)	Feb 22, 2021 6:18 PM	Mar 23, 2021 9:16 PM
<input type="checkbox"/> nicks case	McNamara, Gavin (CONTRACTOR) (1...	Feb 22, 2021 5:43 PM	Mar 23, 2021 9:16 PM
<input type="checkbox"/> subset sharing	McNamara, Gavin (CONTRACTOR) (1...	Feb 18, 2021 12:29 AM	Mar 23, 2021 9:16 PM
<input type="checkbox"/> [EXTERNAL SHARE 145857] auto-gene...	Gavin, McNamara (183374)	Mar 11, 2020 12:46 PM	Mar 19, 2021 4:24 PM
<input type="checkbox"/> [EXTERNAL SHARE 73680] auto-gene...	Gavin, McNamara (183374)	Mar 10, 2020 2:26 PM	Mar 19, 2021 4:24 PM
<input type="checkbox"/> [EXTERNAL SHARE 180510] auto-gene...	Gavin, McNamara (183374)	Mar 16, 2020 8:40 PM	Mar 19, 2021 4:24 PM
<input type="checkbox"/> [EXTERNAL SHARE 202140] auto-gene...	Gavin, McNamara (183374)	Mar 16, 2020 10:20 PM	Mar 19, 2021 4:24 PM

The Grant Access screen is shown on the right side of the page.

4. Select how the access lists for the selected case files are affected:

Manage access inside my agency 1 File

Access Settings

ACCESS L... DURATION

Role Until Removed

Access List

USER OR GROUP

234567

Buonasera, Bradford (234567) bbuonasera@axon.com

Fash, Nicholas (CONTRACTOR) (155235)

CANCEL ADD

5. From the **Access Level** list, select the access level for the user.

- If **Role** is selected, the actions a user can take on the case and evidence in the case depends on the permissions associated with their assigned role.
- If **View** is selected, the user can only view the case and the evidence in the case.

6. From the **Duration** list, select the period of time the user can access the case.

The default value is Until Removed, which means access to the case is granted until the user or group is manually 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. A list of matching users or groups will be displayed as you enter the search criteria. 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** icon.

8. Repeat step 7 to add other users and groups.
9. Click **Save**.
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 cases.

Modifying an Inside My Agency Case Access List

You can modify the access duration and the access level for users and groups on the Case Access Control List from the Case Details Page.

Note: This procedure can be used to modify access information for a Case with a Restricted or Confidential access class.

1. On the case Detail page, click **Manage Access**.

The screenshot shows the Case Details page for 'nicks case3'. The page has a top navigation bar with a 'BACK TO CASES' link and a timestamp 'Last updated: Mar 23, 2021 9:16 PM by Fash, Nicholas (CONTRACTOR) (155235)'. The main content area is divided into two tabs: 'SUMMARY' and 'EVIDENCE (11)'. The 'SUMMARY' tab is active, showing case details like 'CASE ID', 'CASE STATUS', 'OWNER', 'RETENTION', and 'TAGS'. On the right side, there is a 'Manage Access' section with a red box highlighting it. This section shows '106' users with an 'EDIT' link. Below it, there is a 'Manage Shares' section showing '1' share with a 'SHARE' link.

The Manage Access screen is shown on the right side of the page.

2. In the access list, click the edit icon on the same line as the user or group you want to modify.

Manage Access ×

ACCESS LIST VIEW ANY
4 0 106 Restricted

Access Class
Access class permissions are determined by system administrator

☐ Unrestricted ☒ Restricted ☐ Confidential

Add to access list

USER OR GROUP

NAME	MEMBERS	ACCESS TYPE	DURATION	ADDED ON	
Cohen, Griffin (112233)		Manual	Until Removed	Mar 25, 2021	
Buonasera, Bradford (234567)		Manual	Until Removed	Mar 25, 2021	
Fash, Nicholas (CONTRACTOR)		Manual	Until Removed	Mar 25, 2021	
MAC, GMAC (8675309)		Manual	Until Removed	Mar 25, 2021	

3. Select the access level and duration as needed.

Manage Access ×

ACCESS LIST VIEW ANY
4 0 106 Restricted

Access Class
Access class permissions are determined by system administrator

☐ Unrestricted ☒ Restricted ☐ Confidential

Add to access list

USER OR GROUP

NAME	MEMBERS	ACCESS TYPE	DURATION	ADDED ON	
Cohen, Griffin (112233)					
Buonasera, Bradford (234567)		Manual	Until Removed	Mar 25, 2021	
Fash, Nicholas (CONTRACTOR)		Manual	Until Removed	Mar 25, 2021	
MAC, GMAC (8675309)		Manual	Until Removed	Mar 25, 2021	

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 **Done** to return to the case Detail page.

Removing Users and Groups from the case Access List

Users can only be removed from the Case Access List for a given case from the Case Details Page.

Note: This procedure can be used to remove users from the access list for case with a Restricted or Confidential access class.

1. On the case Detail page, click **Manage Access**.

The screenshot displays the Axon Evidence Case Details page for 'nicks case3'. The page includes a header with a 'BACK TO CASES' link and a 'Last updated' timestamp. The main content area is divided into a left sidebar with tabs for 'SUMMARY' and 'EVIDENCE (11)', and a right sidebar with 'Manage Access' and 'Manage Shares' sections. The 'Manage Access' section is highlighted with a red box, showing '106' users and an 'EDIT' link. The 'Manage Shares' section shows '1' share and a 'SHARE' link.

PRIMARY CASE ID	CASE STATUS	OWNER	RETENTION	TAGS
nicks case3	Active	MAC, GMAC (8675309)	Longest Retention Period	

The Manage Access screen is shown on the right side of the page.

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

Manage Access

ACCESS LIST VIEW ANY
4 0 +06 Restricted

Access Class
Access class permissions are determined by system administrator

☐ Unrestricted ☒ Restricted ☐ Confidential

Add to access list

USER OR GROUP
Enter name, email address, or badge ID

NAME	MEMBERS	ACCESS TYPE	DURATION	ADDED ON
Cohen, Griffin (112233)		Manual	Until Removed	Mar 25, 2021
Buonasera, Bradford (234567)		Manual	Until Removed	Mar 25, 2021
Fash, Nicholas (CONTRACTOR)		Manual	Until Removed	Mar 25, 2021
MAC, GMAC (8675309)		Manual	Until Removed	Mar 25, 2021

The user or group 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 case.

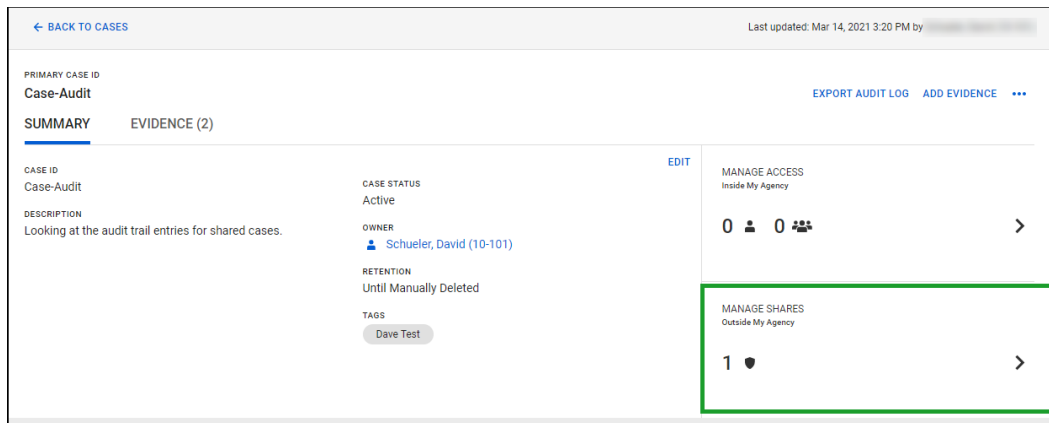
3. Repeat step 2 to remove other users and groups from the list.
4. When you have finished removing users, click **Done** to return to the case Details page.

Sharing Cases Outside Your Agency

You can case information two ways:

- Sharing the case with a partner agency. This creates a copy of the case in the partner agency's instance of Axon Evidence. Shared cases can be updated when evidence is added.
- Sending a download link with the case information. Note that the link can be used by anyone who receives it, not just users in a partner agency.

The Manage Shares section on the Case Details page shows how many times the case has been shared outside of your agency.



Shared Case Retention Information

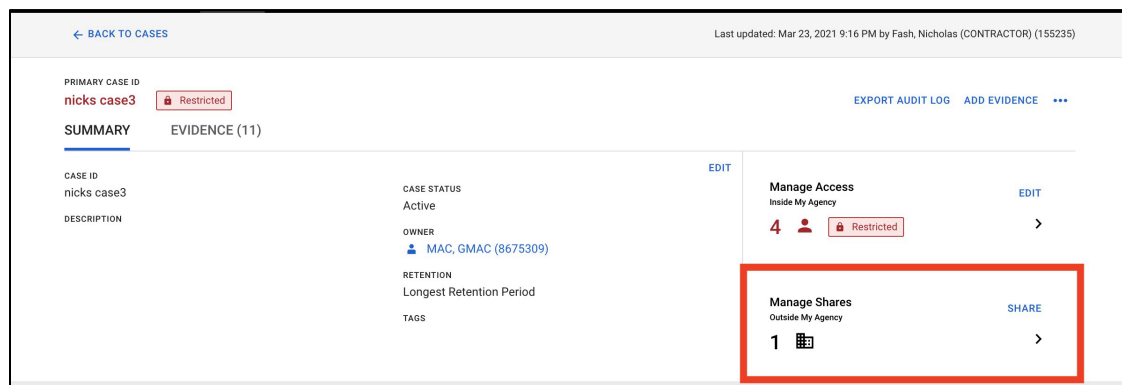
When evidence is shared to your agency as part of a partner case share, the following retention rules are applied:

- Categories are set to None (uncategorized) for all evidence shared to your agency as part of a partner agency case share.
- If your agency has Configurable Case Retention Policies enabled, then the shared case is created using your agency's default retention policy. Users with the Edit Case Retention permission can change the case retention.
- If your agency does not have Configurable Case Retention Policies enabled, then all evidence in a case is kept until manually deleted.

Share Case to Users or Groups Within a Partner Agency

On the Case Detail page, the Manage Shares section shows the number of partner agencies the case has been shared with. The case can be shared with additional partner agencies by accessing the Manage Shares page.

1. On the Case Detail page, click **Manage Shares**.



The Manage Shares screen is shown.

2. Click **New Share**.

The Case Share Details page is shown.

Note: When sharing a Case to Partner Agency, the user must select the partner agency and Users or Groups at the partner agency will receive the case share.

3. Select add **Partner Agency**

The screenshot shows the 'Case Share Details' page. At the top, there is a navigation bar with 'Share Case' and two tabs: '1. Case Share Details' and '2. Select Evidence'. The main heading is 'Case Share Details' with a subtext: 'Select agency to share to and any information to share in addition to the evidence.' Below this, there is a 'PARTNER AGENCY' section with a list of agencies. The first agency, 'NYPD-DA-TEST', is selected and highlighted. Other agencies listed include 'Staten Island District Attorney's Office - NY', 'Brooklyn District Attorney's Office', 'Taser Test Agency 01', 'CCRB-NYC', and 'NYC Law Department'. To the right of the agency list is an 'ATTACHMENTS' section with a list of items: 'Notes', 'Clips', 'Markers', 'Audit Trails', and 'Transcripts'. Each item has a checked checkbox. At the bottom right of the agency list, there is a pagination indicator '0/1024'.

PARTNER AGENCY
NYPD-DA-TEST
Staten Island District Attorney's Office - NY
Brooklyn District Attorney's Office
Taser Test Agency 01
CCRB-NYC
NYPD-DA-TEST
NYC Law Department

ATTACHMENTS
<input checked="" type="checkbox"/> Notes
<input checked="" type="checkbox"/> Clips
<input checked="" type="checkbox"/> Markers
<input checked="" type="checkbox"/> Audit Trails
<input checked="" type="checkbox"/> Transcripts

4. Select Add User or Group.

The screenshot shows the 'Case Share Details' form. At the top, there are two tabs: '1. Case Share Details' (active) and '2. Select Evidence'. The form title is 'Case Share Details' with a subtitle 'Select agency to share to and any information to share in addition to the evidence.' Below this, there are two main sections: 'PARTNER AGENCY' and 'USER OR GROUP'. The 'PARTNER AGENCY' section has a dropdown menu with 'NYPD-DA-TEST' selected. The 'USER OR GROUP' section has a search bar with 'Select...' and a list of results. The results list includes 'DA Test NYPD-DA-TEST' (highlighted), 'Diaz, Juan Carlos (444444) NYPD-DA-TEST', 'Fash, Nicholas (111111) NYPD-DA-TEST', and 'Group Test NYPD-DA-TEST'. To the right of these sections is an 'ATTACHMENTS' section with five checkboxes: 'Notes', 'Clips', 'Markers', 'Audit Trails', and 'Transcripts', all of which are checked.

Section	Item
PARTNER AGENCY	NYPD-DA-TEST
USER OR GROUP	Select...
	DA Test NYPD-DA-TEST
	Diaz, Juan Carlos (444444) NYPD-DA-TEST
	Fash, Nicholas (111111) NYPD-DA-TEST
	Group Test NYPD-DA-TEST

ATTACHMENTS
<input checked="" type="checkbox"/> Notes
<input checked="" type="checkbox"/> Clips
<input checked="" type="checkbox"/> Markers
<input checked="" type="checkbox"/> Audit Trails
<input checked="" type="checkbox"/> Transcripts

- In the **User or Group** field, start typing the name, badge ID, or email address of the user or the name of the group. Axon case 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.

Note: The user must be an active member of a Partner Agency for the case to be shared to them

5. In the **Attachments** section, select the check boxes for the attachments that you want to give to the users/groups you are sharing with.

The screenshot displays the 'Share Case' interface with two tabs: '1. Case Share Details' and '2. Select Evidence'. The 'Case Share Details' section includes a dropdown for 'PARTNER AGENCY' (NYPD-DA-TEST), a dropdown for 'USER OR GROUP' (Select...), and a list of users/groups (DA Test, Fash, Nicholas) with remove icons. A 'MESSAGE' field contains the text 'Friendly Message to Recipient'. On the right, the 'ATTACHMENTS' section is highlighted with a red box, showing five checked items: Notes, Clips, Markers, Audit Trails, and Transcripts.

- Notes - Case & Evidence Notes
- Clips - Evidence Clips
- Markers - Evidence Markers
- Audit Trails — User can view the audit trail of the case and all evidence included in the case share
- Transcripts - Transcripts that previously have been created for evidence included in the case share

6. Click **Next** to continue to the next step to share Case to Partner Agency

The screenshot shows the 'Case Evidence' interface. At the top, there's a header with a tag 'Solar_Orbiter_s_first_views_of_th...' and user 'McNamara, Gavin (CONT...' with a count of 124. Below this, a message states 'ID This is a new Tag', 'RECORDED ON Feb 4, 2021 6:59 PM', and 'CATEGORY None'. The main section is titled 'Case Evidence' with '11 results | 5 selected'. A red box highlights the 'ADD TO CASE SHARE' button. Below this, there are 'Folders' (gavin 2/22/2..., nicks folder) and 'Quick Views' (RESET). The 'Quick Views' section lists 'FILE TYPE' (Image: 6, Video: 5) and 'RECORDED BY' (624867 Baid, Sonal: 5, 124485 McNamara, Gavin (CON TRACTOR): 3). The main table lists evidence items with columns: ID, TITLE, OWNER, UPLOADED BY, UPLOADED ON, RECORDED ON, CATEGORY, and STATUS. The table shows several items, including 'nick mobile dems hgiehg ON Body 2...', 'DEMO', 'Tag testing', and 'This is a new ...'. At the bottom, there are buttons for 'CANCEL' and 'SHARE CASE'.

- Select which pieces of evidence to share to the partner agency
- Once the evidence is selected, click **Add to Case Share**, then **Share Case** on the Bottom right of the page

The screenshot shows a success message dialog box. At the top, there's a green checkmark icon. The text inside the box reads: 'You have successfully initiated sharing this case with NYPD-DA-TEST. Share recipients will receive an email after the evidence has been copied into their agency. This may take several hours depending on the amount of evidence shared.' At the bottom, there is a blue button labeled 'CLOSE'.

7. The system shows that the case has been successfully initiated for sharing. The recipient will receive an email once the case share completes.

Note: All cases shared to partner agencies are automatically created in the partner agency's Axon Evidence account with the Unrestricted access class. However, the case share recipient may choose to update the case's access class at any time. Once the case's

access class have been updated, all evidence that is shared into the case via a case share update will be automatically created with the case's current access class.

Updating a Shared Case

If you add evidence to a case that has already been shared to a partner agency, you can choose to update the case share when adding the new evidence or you can update the case share through the Case Details page after the evidence is added.

Updating the case share while adding evidence will share all the newly added evidence to a partner agency, while updating the case share after adding evidence allows you to select which evidence is added to the case share.

In both situations, the evidence will be added to the partner agency's copy of the case and they will receive an email notifying them that new evidence has been added.

Updating a Shared Case when Adding Evidence

After adding evidence to a case you have the option to update the case share for all partner agencies to include the newly added evidence.

The image displays two side-by-side screenshots of the 'Add to Case' interface. Both screens show a success message 'Evidence Added To Case' with a green checkmark icon. Below this, there is a checkbox labeled 'Update case share with listed partners'. In the left screenshot, this checkbox is unchecked, and the button at the bottom is labeled 'FINISH WITHOUT SHARING'. In the right screenshot, the checkbox is checked, and the button at the bottom is labeled 'SHARE AND FINISH'. Both screens also display a list of partners under the heading 'This case has previously been shared with these partners:', with 'Spurbury PD' listed as a partner.

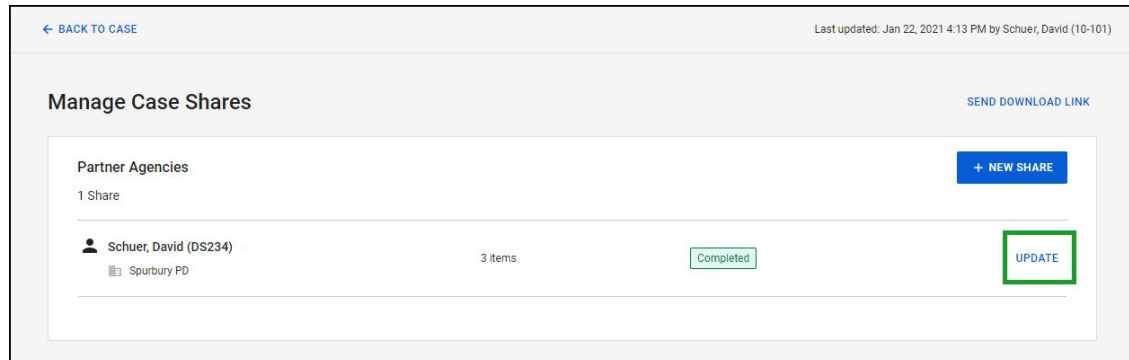
- To add the evidence to a case without updating the case share, click **Finish without sharing**.
- To update the case share for with the newly added evidence for the listed partner agencies, select **Update case share with listed partners** and click **Share and Finish**.

Updating a Shared Case after Evidence is Added

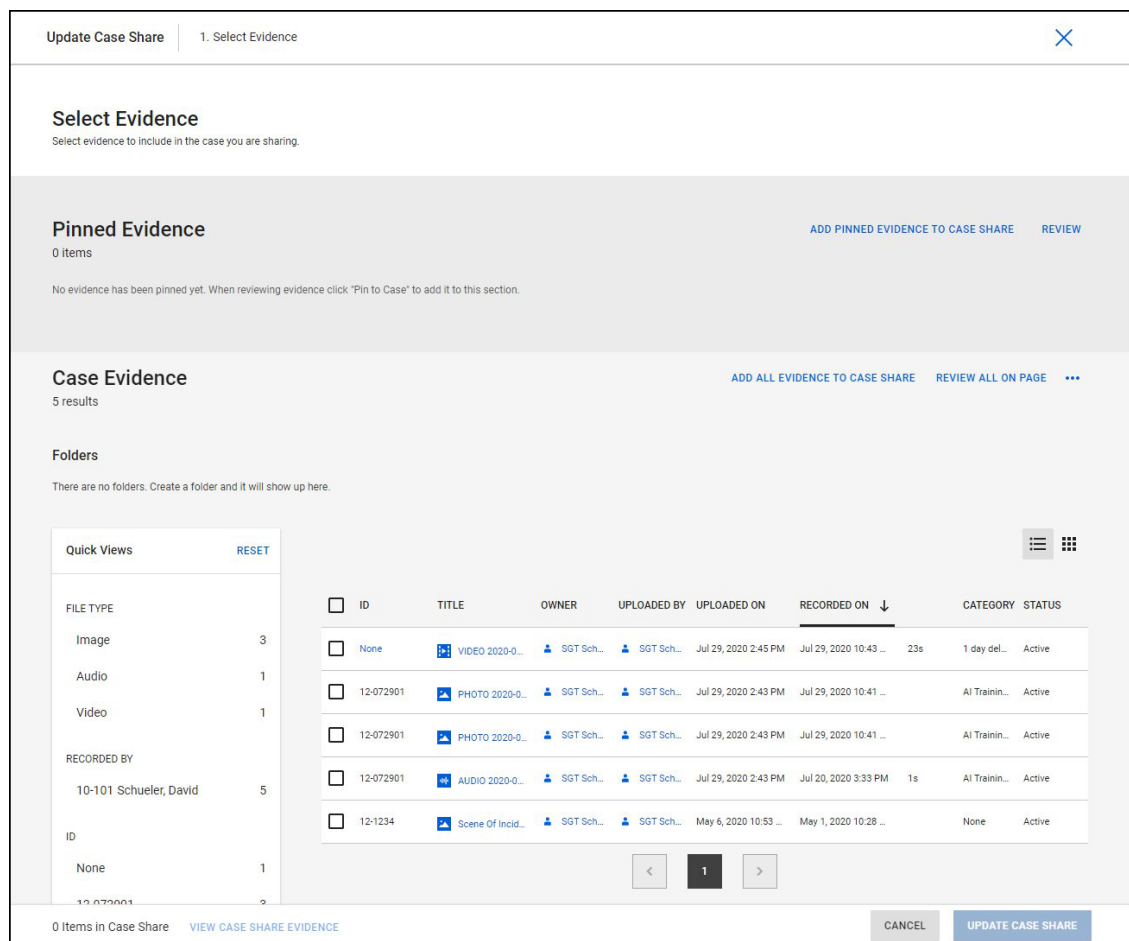
If you did not update case shares when evidence was added to the case, you can do so at a later time from the Case Details page.

1. Open the Case Details page for the case.
2. On the Case Details page, click **Manage Shares**.

- On the Manage Case Shares page, Click **Update** for the partner agency case share you want to update.



- Select the evidence you want to add to the partner agency case share.



There are several options available for sharing evidence. You can:

- Click **Add All Evidence to Case Share** to share all evidence in the case.

- Click **Add Pinned Evidence to Case Share** to add all pinned evidence to the case share.
- Select evidence and click **Add to Case Share** to add the selected evidence to the case share.
- View evidence in the review mode and click **Add Evidence to Case Share**, in the upper right of the review mode, to add the evidence to the case share.
- Open a folder and click **Add Folder to Case Share** to add all evidence from the folder into the case share.

Note: When evidence in a folder is added to the case share, the folder is also included.

Example: A case has three folders - Folder A with Evidence 1, Folder B with Evidence 1 and Evidence 2, and Folder 3 with Evidence 3. If Evidence 1 and Evidence 3 are added to the case share, the partner agency's copy of the case will contain Folder A with Evidence 1, Folder B with Evidence 1, and Folder C with Evidence 3.

5. After you have selected the evidence, review the information to verify it is correct.

Click **View Case Share Evidence** to see the new evidence that has been added to the case share. Click **Back to Select Evidence** to return to the Select Evidence page.

If you need to add more evidence, repeat step 4 as needed.

6. Click **Update Share Case**.

Axon Evidence will update the partner agency's case share with the evidence you have selected. The user(s) or group(s) with which the case was shared to will be notified via email that new evidence has been shared once the update has completed successfully.

7. After you have finished sharing, click **Back to Case** to return to the Cases Detail page.

Send a Download Link

1. On the Case Details page, click the Manage Shares tile.

2. On the Case Sharing page, click **Send Download Link**.

← BACK TO CASE Last updated: Dec 17, 2020 9:04 PM by Stevens, Shawn (ss007)

Manage Case Shares

SEND DOWNLOAD LINK

Partner Agencies

0 Shares

+ NEW SHARE

Name	Duration	Status
No Shares Added		

Add by selecting the Share or Send Download Link action above.

3. On the Download Link Details page:

Send Download Link 1. Send Download Link

Download Link Details

Select recipient to share to and any information to share in addition to the evidence.

USER OR EMAIL ADDRESS *

Enter Name, Badge, or Email Address

MESSAGE

Send a friendly message

0/1024

ATTACHMENTS

☐ Audit Trails

☐ Table of Contents

☐ Transcripts

PACKAGE TYPE

☒ ZIP

☐ ISO

DURATION (DAYS)

3

CANCEL SEND DOWNLOAD LINK

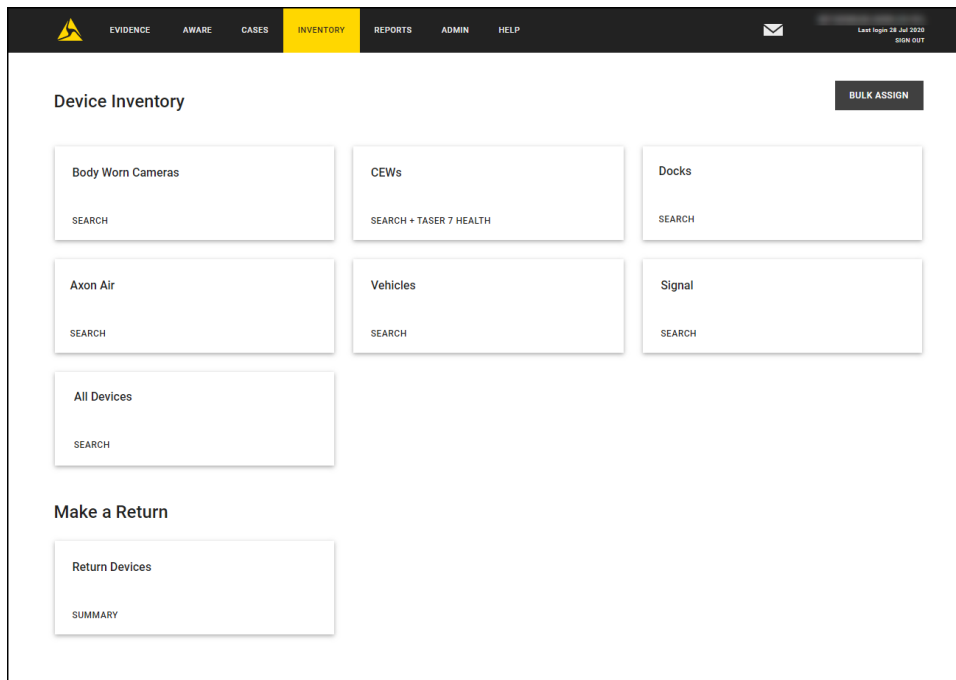
4. In the **User or Email Address** field, add the users or email addresses you want to send the download link to as follows:
 - For a user in your agency or a partner agency, start typing the name of the user, wait for Evidence.com to show the matching users, and then click the user you want. You can 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**.

5. Select any additional information to include:
 - Selecting **Audit Trails** will share all of the audit events for the case and evidence in the case with the partner agency.
 - Selecting **Table of Contents** adds a Microsoft Excel spreadsheet to the download with the following fields: File Name, Evidence ID, Evidence Title, File Type, File Size, Evidence Duration, Date Recorded, Uploader-First Name, Uploader-Last Name, Uploader-Badge ID, Assignee-First Name, Assignee-Last Name, Assignee-Badge ID, and Agency Name.
 - Selecting **Transcripts** will share all the all the human generated and Axon Auto-Transcribe transcripts associated with the case.
6. Select the Package Type, **ZIP** or **ISO** file. This is the type of file the download link recipient can download.
7. In the **Duration** field, type the number of days that the evidence link is to be available.
8. Review that the information is correct, then click **Send Download Link**.
9. A link for downloading the file is sent to the user or email you added. The files will only be available until the duration you specified expires.

After you have finished sharing, click **Back to Case** to return to the Cases Detail page.

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, 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.

- **Return Devices** – Opens the Axon Evidence Device Return Service to let users with the appropriate permission start the return process or check the status of devices returned to Axon. See the [Returns section](#) of this guide for more information.

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**.

Note: If your agency has TASER 7 devices, you are taken to the TASER 7 Health page when you click **CEWs**. Click **CEW Search** to go to the CEW search page.

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.

Task	Steps
Find devices assigned to you or another person.	In the Assigned To field, enter the name of person whose devices you want to see.
Find unassigned devices.	In the Device Status filter, select In Stock .
Change search results	Update the device search filters or click Reset Filters . For more information, see Device Search Filters .
Sort search results	<p>Use the Sort By list to select a column and click Sort Order to change order.</p> <p>Click the column heading for Serial Number, Device Name, Last Upload, Device Status, Error Status, Firmware, or Warranty. To reverse the sort order, click the heading again.</p>

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 **x81**, the search results would include devices with the serial numbers **X81162367** and **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.
- **Device Home** — Limits the search to devices that are assigned to a specified Device Home or None.

Note: The Device Home attribute is only shown on the Inventory search page if your agency has at least one Device Home.

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 **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.

UPDATE STATUS

EXPORT

71

ITEMS FOUND

SORT BY

Last Upload

SORT ORDER

Az ↑

Za ↓

<input type="checkbox"/>	MODEL	SERIAL NUMBER	DEVICE NAME	ASSIGNEE	LAST UPLOAD ↓	DEVICE STATUS	ERROR STATUS	FIRMWARE	WARRANTY
<input type="checkbox"/>	Axon Body 2	X81199528	X81199528	None	Jun 27, 2018 12:31 PM	In Stock	Good	1.15.2	None
<input type="checkbox"/>	Axon Body 2	x81002515	X81002515	None	Dec 18, 2017 3:24 PM	In Stock	Good	1.11.16	None
<input type="checkbox"/>	Axon Body 2	X81065867	X81065867	None	Oct 12, 2017 5:55 PM	In Stock	Good	1.11.16	None
<input type="checkbox"/>	Axon Body 2	X81175860	X81175860	None	Aug 31, 2017 4:25 PM	In Stock	Good	1.11.4	None
<input type="checkbox"/>	Axon Body 2	x81003582	X81003582	None	Jun 12, 2017 3:42 PM	In Stock	Good	1.8.85	None
<input type="checkbox"/>	Axon Body 2	X81136326	X81136326	None	May 17, 2017 7:37 AM	In Stock	Good	1.9.149	None
<input type="checkbox"/>	Axon Body 2	X81066067	X81066067	None	May 15, 2017 8:27 A...	In Stock	Good	1.9.149	None
<input type="checkbox"/>	Axon Body 2	x81042809	x81042809	None	Mar 30, 2017 1:48 PM	In Stock	Good	1.9.128	None
<input type="checkbox"/>	Axon Body 2	x81000839	X81000839	None	Mar 10, 2017 2:58 PM	In Stock	Good	1.8.86	None
<input type="checkbox"/>	Axon Body 2	x81002615	X81002615	None	Sep 12, 2016 5:15 PM	In Stock	Good	1.1.59	None
<input type="checkbox"/>	Axon Body 2	x81000917	X81000917	None	May 20, 2016 3:49 ...	In Stock	Good		None

Update Device Status

Users with Device Administration permission can change the status, including unassigning devices, for selected devices. Most Axon devices can also be assigned, unassigned, and have the status changed 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 select the new status from the list.

Update Status

12
Selected

Select Status

In Stock

Lost

Stolen

Review

RMA

Scrapped

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.

- 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.

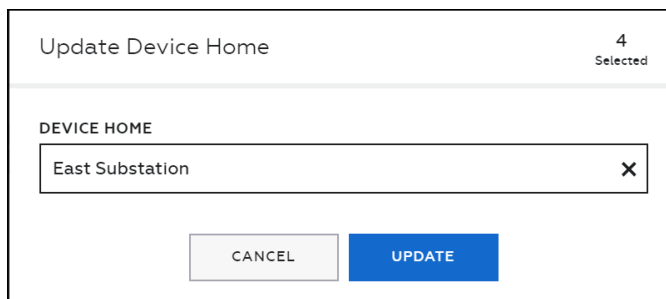
Status	Description
Assigned	This device has been assigned to a user in your agency.
In Stock	This device has been registered to your agency, but not assigned to a user.
In Evidence	This device is registered to your agency and is being held as physical evidence and has been withdrawn from deployment.
In Test	This device is registered to your agency and is undergoing standard test and maintenance procedures.
Lost	This device is registered to your agency and has been reported as lost.
Stolen	This device is registered to your agency and has been reported as stolen.
Review	This device is registered to your agency and is currently undergoing investigation/troubleshooting.
RMA	This device is registered to your agency and has been returned to Axon for RMA processing.
Relinquished	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.
Scrapped	This device is registered to your agency and has been reported as destroyed or no longer serviceable.

Update Device Home

Note: The Device Home attribute is only shown on the Inventory search page if your agency has at least one Device Home.

Users with Device Administration permission change the Device Home for selected devices. Device Home information is included in the Device Summary report.

1. Search for the device or devices.
2. Select the devices in the search results
3. Click **Update Home** and select the Device Home from the list.



Update Device Home 4 Selected

DEVICE HOME

East Substation X

CANCEL UPDATE

4. Click **Update**.

The system confirms the Device Home is assigned. Click **Close** to return to the search page.

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.

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, CSV, or Microsoft Excel 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 information and actions available on the Device Profile page.



TASER X26P


STATUS: ASSIGNED [✎](#)

DEVICE NAME:
ZZX1201Y2 [✎](#)

DEVICE HOME:
HOME3 [✎](#)

AUDIT TRAIL





User Information


ASSIGNEE	ASSIGNED SINCE	
 Stevens, Erik (3424343)	Feb 28, 2019	REASSIGN

Summary

MODEL	SERIAL NUMBER	WARRANTY	FIRMWARE
TASER X26P	ZZX1201Y2	—	04.037

Recent Evidence | [View All](#)

ID	TITLE	OWNER	UPLOADED ON	STATUS
None	 TASER X26P CEW Log 2019-02-28 114	 Stevens, Erik (3424343)	Feb 28, 2019 11:49 AM	Active
None	 TASER X26P CEW Log 2019-02-28 105	 Stevens, Erik (3424343)	Feb 28, 2019 10:52 AM	Active



Axon Body 2

STATUS: IN STOCK [✎](#)

DEVICE NAME:
XB1235242 [✎](#)

DEVICE HOME:
NONE [✎](#)

AUDIT TRAIL

User Information

ASSIGNEE	ASSIGNED SINCE	
None	—	REASSIGN


Summary

MODEL	SERIAL NUMBER	WARRANTY	FIRMWARE
Axon Body 2	XB1235242	—	1.17106

State

TITLE	DESCRIPTION	LAST UPDATE
Host Recent Dock	Name: X79017403 Serial: X79017403	May 16, 2019 4:35 PM

Recent Evidence | [View All](#)

ID	TITLE	OWNER	UPLOADED ON	STATUS
None	 AXON Body 2 Video 2019-04-29 1330	None	May 6, 2019 8:25 AM	Active

Device Settings

SPEAKER VOLUME
Controls volume of camera audio prompts.

☐ High
☒ Medium
☐ Low
☐ Off

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

☒

INDICATOR LIGHTS
Controls whether the camera Event/Battery LED emits light during operations. Stealth must be disabled for this setting to be enabled.

☒

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

☐

SAVE SETTINGS

The Device Profile page is divided into several sections. Not all sections are used for all devices.

- The left side of the profile page shows the current device status, name, device home information, and provides access to the device audit trail.
- The User Information section shows the current assignee, when the device was assigned to the user, and provides access to reassign the device.
- The Summary section shows essential information about the device, such as the firmware version and warranty information.
- The State section includes information about the most recent Axon Dock connection for the device. 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 information to Evidence.com.
- The Connected Devices section is only shown for Docks. It provides information on devices, such as body worn cameras and TASER 7 batteries, that are currently in the Dock.
- The Recent Evidence section lists and provides links to evidence recently uploaded from the device. Clicking on the evidence title takes you to the Evidence Detail Page for the evidence.
- The Device Settings section shows the user settings for the device. The settings that can be changed depend on the type of device and agency-level device 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, in the User Information section, click **Reassign**.

The Reassign Device dialog is shown.

2. In the name or badge ID field, 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 or select the user from the list.

3. Click **Reassign**.

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 in the Recent Evidence section. This list includes videos recorded by Axon body worn cameras and CEW firing logs.

1. On the Device Profile page, scroll to the **Recent Evidence** section.

If the evidence you are looking for is not shown, click **View All** to go to the Evidence Search page for the device.

2. Use the evidence list as needed. The following table provides steps for the tasks you can perform from the evidence list.

Task	Steps
View, edit, download, or flag/un-flag 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.

Edit Device Settings

The device settings that can be changed depend on the type of device and agency level device settings.

- For Axon Body 3 cameras, you can edit the device name, configure the speaker volume, configure camera vibration, camera indicator lights, camera LED automatic brightness, and whether the camera is in stealth mode.
- 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 Axon Flex cameras, you can edit the device name and orientation.
- For other device types, you can change the device name.

1. On the Device Profile page, scroll to the Device Settings section.
2. Edit the settings as needed.
3. Click **Save Settings**.

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 Profile page is shown.

4. On the left side of the Device Profile page, 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.

TASER 7 Health

The TASER 7 Health page tracks the status of your agency's TASER 7 and TASER 7 CQ devices, cartridges and batteries.

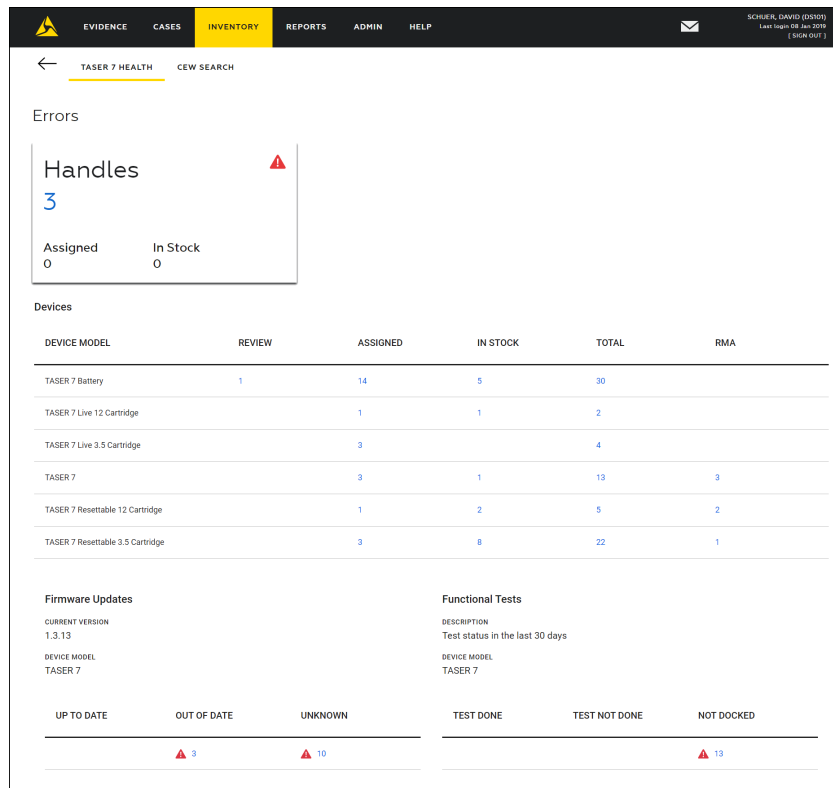
1. On the menu bar, click **Inventory**.
2. Click **CEWs**.

The TASER 7 Health page is shown. The page is divided into four sections – Errors, Devices, Firmware Updates, and Functional Tests.

- The Errors section shows the TASER 7 items that are in an error state. If no items are in an error state, this section is blank.
- Devices lists the number of TASER 7 device models by status.
- Firmware Updates shows the current firmware version and the number of devices that are up to date or out of date.

- Functional Tests shows the functional test status for TASER 7 CEWs in the past 30 days. Users need to perform a functional test and then dock the battery to update status in this dashboard. Devices that have not been docked in the past 30 days are shown in the NOT DOCKED column.

Clicking on a number opens a filtered search results page with only the items that fall into the clicked grouping shown (*example:* Clicking the number shown in the TASER 7 In Stock column will open a search results page showing all TASER 7 handles with a status of In Stock.)



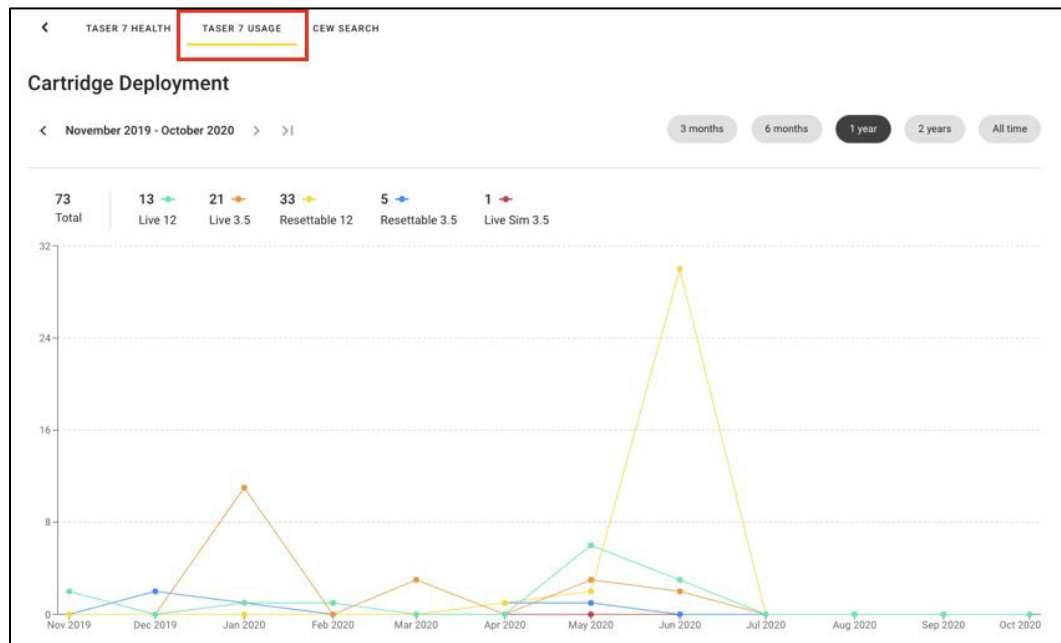
TASER 7 Usage Dashboards

The TASER 7 Usage dashboards are designed to help you better understand device usage in your agency. The dashboards are available to customers on OSP7 plans and TASER 7 Certification plans.

The first dashboard we are releasing is the **Cartridge Deployed** dashboard. This dashboard shows the type and number of cartridges deployed by your agency during the selected time.

- On the menu bar, click **Inventory**, click **CEWs**, and then click **TASER 7 Usage**.

2. Select the time range you want to view.



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.

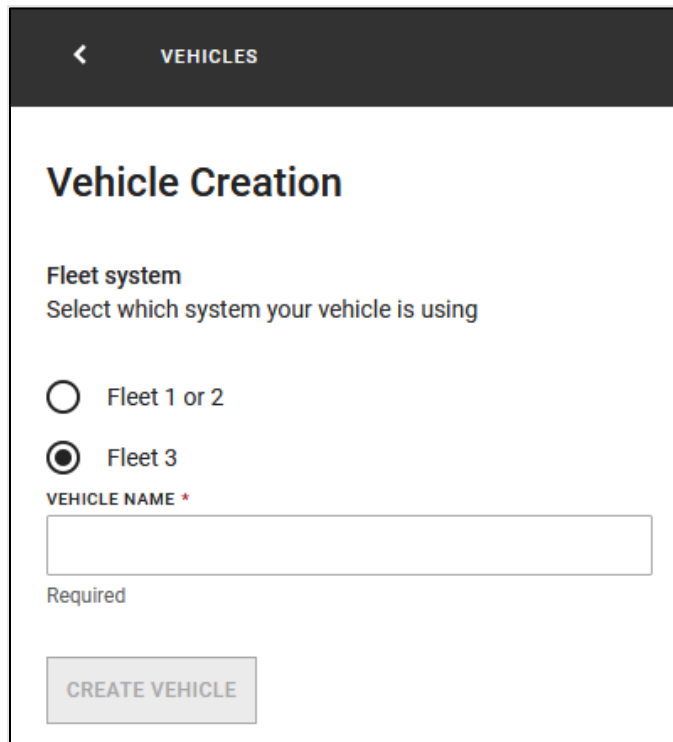
The Vehicle section only available to agencies that use Axon Fleet.

Add a New Fleet 3 Vehicle

1. On the menu bar, click **Inventory** and then click **Vehicles**.

The vehicle page displays a list of vehicles with Axon Fleet systems associated with your Axon Evidence account.

2. Click **Guided Vehicle Creation** and select Fleet 3.



The screenshot shows a mobile application interface for 'VEHICLES'. At the top is a dark header with a back arrow and the word 'VEHICLES'. Below this is a section titled 'Vehicle Creation'. Under the heading 'Fleet system', there is a prompt 'Select which system your vehicle is using'. Two radio button options are present: 'Fleet 1 or 2' (unselected) and 'Fleet 3' (selected). Below the radio buttons is a text input field labeled 'VEHICLE NAME *' with a red asterisk. A 'Required' label is positioned below the input field. At the bottom of the form is a grey button labeled 'CREATE VEHICLE'.

3. Type a Name for the vehicle and click **Create Vehicle**.
4. Click **Assign** in the Fleet Hub row of the Axon Systems.

Note: A feature to assign Signal Vehicle to your Fleet 3 Vehicle will be available after launch.

Axon Systems		
Device	Serial Number	
Fleet Hub	-	ASSIGN
Signal Vehicle	-	ASSIGN

5. Enter the serial number of the Fleet Hub installed in the vehicle and click **Assign**.

A modal dialog box titled "Assign" with a close button (X) in the top right corner. Inside the dialog, there is a section labeled "FLEET HUB" containing a dropdown menu with the text "Select Hub" and a downward arrow. At the bottom of the dialog, there are two buttons: "CANCEL" and "LABEL".

6. If you need to add another vehicle, repeat steps 1 – 5.

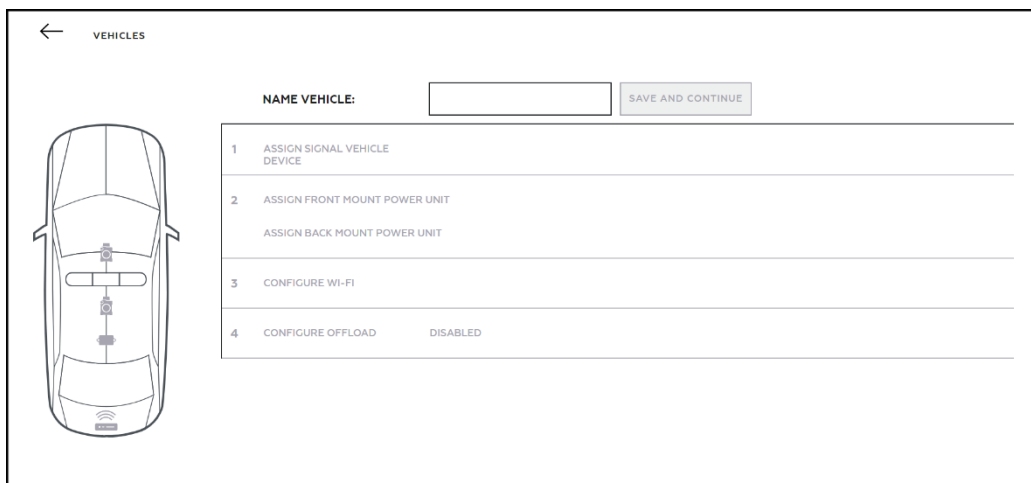
Add a New Fleet 1 or 2 Vehicle

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 **Guided Vehicle Creation** and select Fleet 1 or 2.
3. Type a Name for the vehicle and click **Save and Continue**.

A screen titled "VEHICLES" with a back arrow in the top left. On the left side, there is a top-down diagram of a vehicle with various components labeled. On the right side, there is a form with the following fields:

- "NAME VEHICLE:" followed by a text input field and a "SAVE AND CONTINUE" button.
- A numbered list of steps:
 1. ASSIGN SIGNAL VEHICLE DEVICE
 2. ASSIGN FRONT MOUNT POWER UNIT
ASSIGN BACK MOUNT POWER UNIT
 3. CONFIGURE WI-FI
 4. CONFIGURE OFFLOAD DISABLED

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.

← VEHICLES

VEHICLE Car 54

- 1 Enter the serial number located on the side of the Axon Signal Vehicle device.
NOTE: Axon Signal Vehicle serial numbers start with X87
SIGNAL VEHICLE DEVICE:
SAVE AND CONTINUE
- 2 ASSIGN FRONT MOUNT POWER UNIT
ASSIGN BACK MOUNT POWER UNIT
- 3 CONFIGURE WI-FI
- 4 CONFIGURE OFFLOAD DISABLED

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**.

← VEHICLES

VEHICLE Car 54

- 1 SIGNAL VEHICLE DEVICE X87495959
- 2 Enter the serial numbers for the Axon Fleet Power Units associated with the Fleet Camera Front and Back mounts.
NOTE: Axon Fleet Power Unit serial numbers start with X85
FRONT MOUNT POWER UNIT:
BACK MOUNT POWER UNIT:
SAVE AND CONTINUE
- 3 CONFIGURE WI-FI
- 4 CONFIGURE OFFLOAD DISABLED

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.

Note: The SSID is case-sensitive.

← VEHICLES

VEHICLE Car 54

1	SIGNAL VEHICLE DEVICE	X87495959	
2	ASSIGN FRONT MOUNT POWER UNIT	—	
	ASSIGN BACK MOUNT POWER UNIT	—	
3	WI-FI	Enter unique SSID and password for this vehicle. <div> SSID <input type="text"/> </div> <div> PASSWORD <input type="text"/> <input type="checkbox"/> SHOW PASSWORD </div>	
4	CONFIGURE OFFLOAD	DISABLED	

SAVE AND CONTINUE

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.

← VEHICLES

VEHICLE Alpha-10

1	SIGNAL VEHICLE DEVICE	X87112235	
2	FRONT MOUNT POWER UNIT	X8543210	
	BACK MOUNT POWER UNIT	X8543211	
3	WI-FI	12884ww	
4	WIRELESS OFFLOAD	Enable this feature when uploading evidence from Axon View XL via Wi-Fi or LTE. Disable this feature when manually docking Fleet cameras. <div> <input checked="" type="checkbox"/> </div>	

SAVE AND CONTINUE

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.

Vehicle Name	Signal	Front Mount	Rear Mount	SSID	Password	Wireless Offload
ID444	X87000025	X850000022	X850000023	garage-a	arc-2343x9	
ID447	X87000026	X850000024	X850000025	garage-a	arc-2343x9	TRUE
ID449	X87000027	X850000026	X850000027	garage-a	arc-2343x9	FALSE

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.

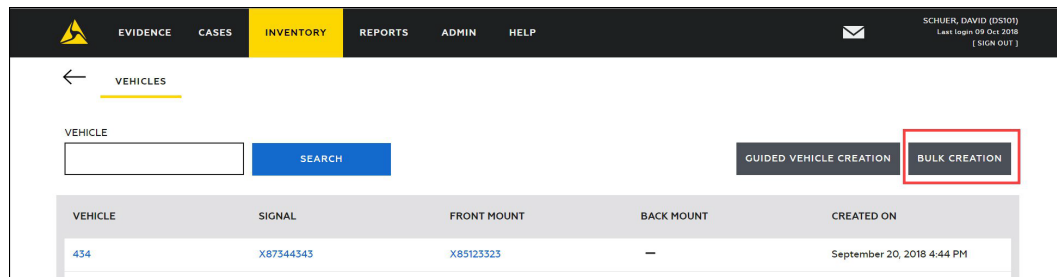
Note: The SSID is case-sensitive.

- **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**.

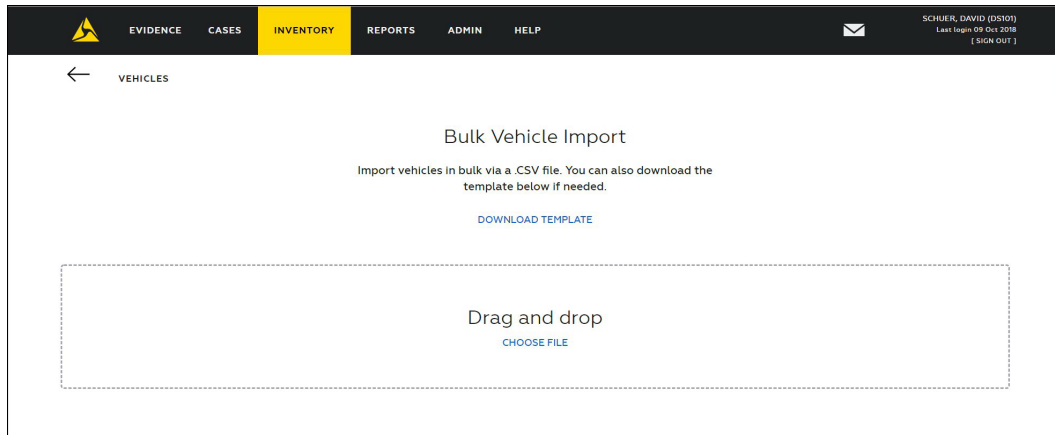
The vehicle page displays a list of vehicles with Axon Fleet systems associated with your Evidence.com account.

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.

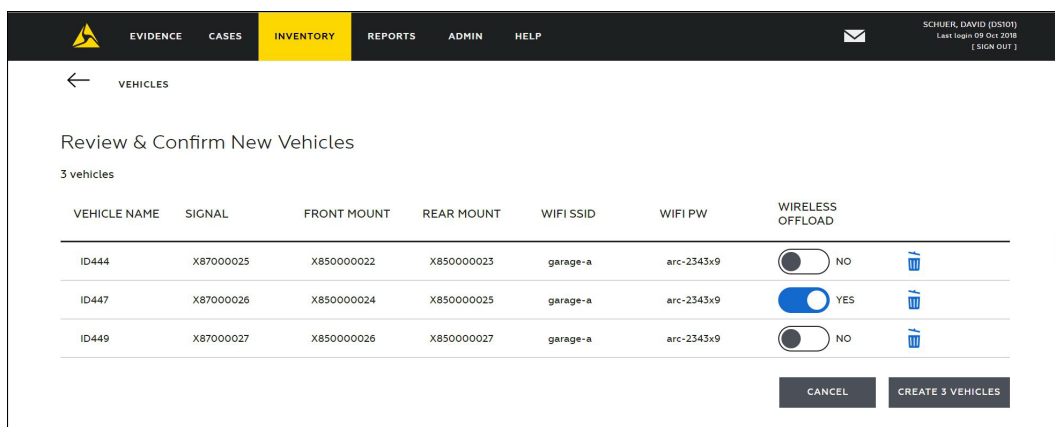
Click **Download Template** to download a copy of the template with dummy data. Delete the dummy vehicle information (row 2) before uploading the csv file.



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 (✎) on the same line as the information you want to change.

Note: The SSID is case-sensitive.

4. Enter the updated information and click **Save and Continue** (or **Save and Complete**).

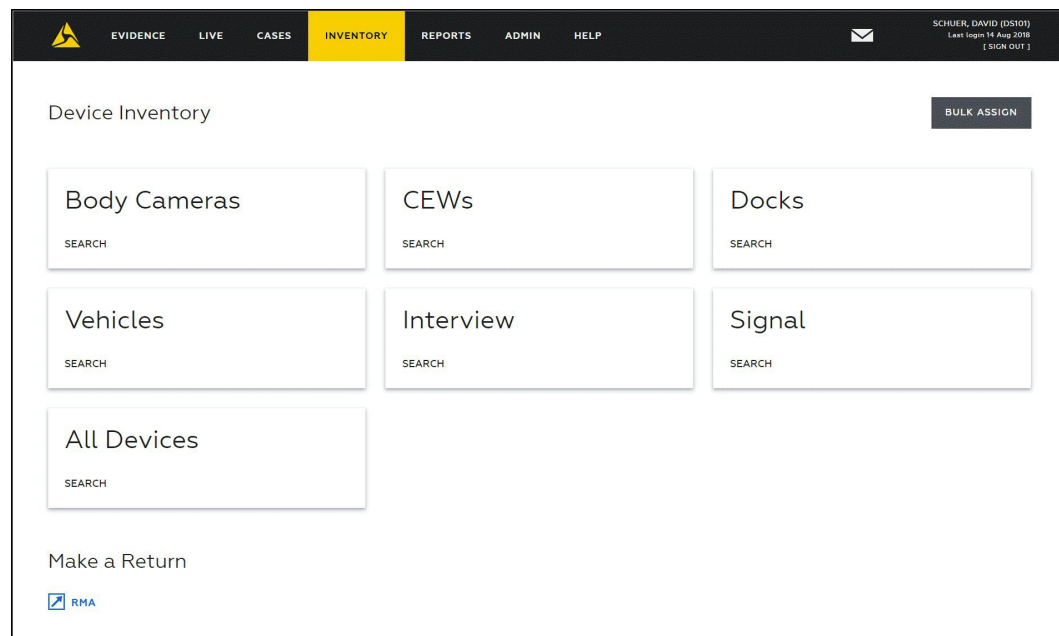
If needed, edit the next set of information.

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.

The screenshot shows the 'INVENTORY' tab selected in the top navigation bar. Below the navigation bar, there is a header section with instructions: 'This feature allows you to quickly assign several devices. Please start typing into the fields below and select from the options that appear.' followed by three bullet points: 'A maximum of ten options will display at a time. Continue typing to reduce the available options.', 'If no options appear after five seconds, please check that the name or serial number is correct.', and 'One user can be assigned multiple devices at once.' Below this, there is a table with two columns: 'Owner' and 'Serial No.'. Each column has five empty text input fields. At the bottom of the table, there are two blue buttons: 'ADD MORE ROWS' and 'ASSIGN DEVICES'.

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 cameras, Axon Flex 2 cameras, and TASER CEWs. Axon Device Manager runs on iOS devices and Android devices that are equipped with an NFC antenna.

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](#).

Returns

The Axon Evidence Device Return Service provides agencies with the ability to manage return merchandise authorization (RMA) requests within Axon Evidence.com. Authorized users will be able to create, update, save, submit, and track device returns for their agency in one place.

Some of the key benefits of Axon Evidence Device Return Service are:

- **Time Savings:** Users do not have to go to multiple systems to submit and track returns, everything is done within Axon Evidence.com. Users can also save in-progress RMA tickets, returning to add more devices at a later time instead of having to restart the process.
- **Accuracy:** Removing the need to manually type long serial numbers means that submitted RMA tickets will be more accurate, allowing returns to be processed more quickly and efficiently.
- **Visibility:** The Returns overview page shows all the RMA tickets an agency has submitted, along with the status of each return. Each return can be expanded individually so that the user can see what items were in the RMA, the reasons for the return, and the tracking status.
- **Convenient Shipping:** Axon Evidence Device Return Service is integrated with FedEx and return shipping labels are provided at no extra charge.

Returns Permissions

Before users can access Axon Returns, they must have the Return Administration permission enabled for their Role.

Note: The pre-configured Admin, Armorer, and Lite Armorer Roles have the Return Administration permission enabled by default.

Agency Evidence.com administrators can modify existing Roles or create new Roles to enable the permission.

The **Return Administration** permission is found in the Admin Access section and must be enabled for users to access the Axon Returns service. Note that the Role must have **User Search** and **Inventory Search** permissions, under Search Access, set to Allowed for the **Return Administration** permission to be available.

Admin Access		
Configure Agency Security Settings	<input type="radio"/> ALLOWED	<input checked="" type="radio"/> PROHIBITED
Edit Agency Settings	<input type="radio"/> ALLOWED	<input checked="" type="radio"/> PROHIBITED
Edit Device Offline & Mic Settings	<input type="radio"/> ALLOWED	<input checked="" type="radio"/> PROHIBITED
CEW Administration (manage and reassign CEWs)	<input type="radio"/> ALLOWED	<input checked="" type="radio"/> PROHIBITED
Device Administration (manage non-CEW devices, reassign devices)	<input type="radio"/> ALLOWED	<input checked="" type="radio"/> PROHIBITED
User Administration	<input type="radio"/> ALLOWED	<input checked="" type="radio"/> PROHIBITED
Category Administration	<input type="radio"/> ALLOWED	<input checked="" type="radio"/> PROHIBITED
Return Administration	<input checked="" type="radio"/> ALLOWED	<input type="radio"/> PROHIBITED
Generate Reports Pro	<input type="radio"/> ALLOWED	<input checked="" type="radio"/> PROHIBITED

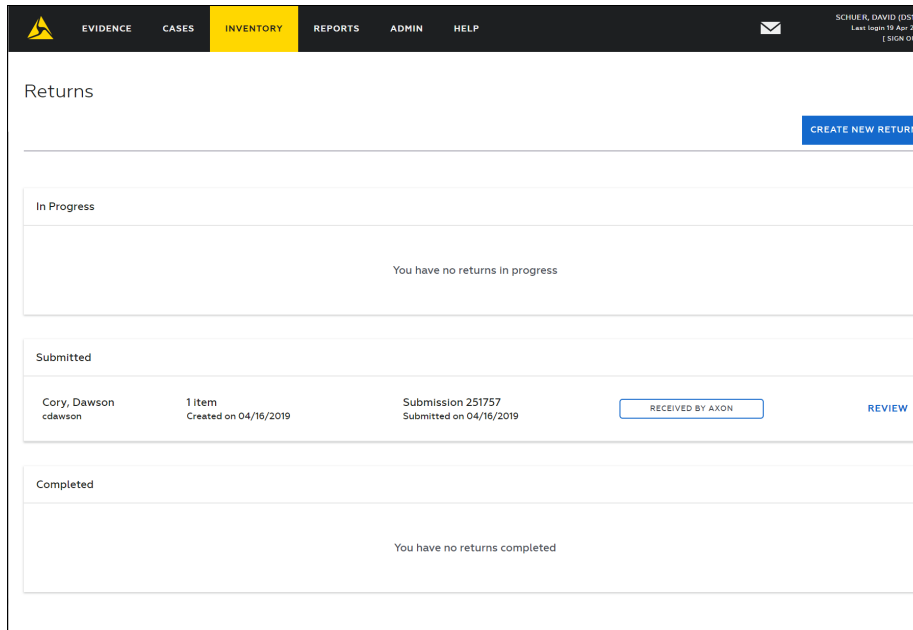
Accessing the Returns Page

1. Sign in to your Axon Evidence account.
2. On the menu bar click **Inventory** and then, under Make a Return, click **Return Devices**.

The screenshot shows the Axon Evidence web application interface. At the top, there is a navigation bar with the following tabs: EVIDENCE, CASES, INVENTORY (highlighted in yellow), REPORTS, ADMIN, and HELP. On the right side of the navigation bar, there is a user profile for 'SCHUBER, DAVID (D5101)' with the text 'Last login 19 Apr 2019' and a '[SIGN OUT]' link. Below the navigation bar, the main content area is titled 'Device Inventory'. On the right side of this section, there is a 'BULK ASSIGN' button. The main content area contains several cards for different device types: 'Body Worn Cameras', 'CEWs', 'Docks', 'Vehicles', 'Interview', 'Signal', and 'All Devices'. Each card has a 'SEARCH' button. Below these cards, there is a section titled 'Make a Return'. Within this section, the 'Return Devices' card is highlighted with a red border. This card has a 'SUMMARY' button at the bottom.

Returns Page Overview

The Returns page is the main page for the Axon Evidence Device Return Service and provides an overview of device returns.



It is divided into three sections:

- **In Progress:** This section lists returns you have started but have not submitted. This section only shows returns started by the user that is signed in.

If you have an In-Progress Return, click **Continue Return** to open the return on the same page where you left off. You can only have one In Progress return at a time.

- **Submitted:** This section lists all agency returns that have been submitted but are not yet complete. Each entry lists the number of items, when the return was submitted, the current status, and provide the option to review the return.
- **Completed:** This section list completed returns for your agency.

For Submitted and Completed Returns, click **Review** to open the Status of Return page for the Return.

The status for each return has a text explanation and a color-coded surrounding box.

- Orange – A user action is required to move to the next step
- Blue – The return is following the normal process
- Black – The return is complete or was canceled

Reviewing Submitted and Completed Returns

The Status of Return page shows the details of the selected return, when it was submitted, and the status.

251757 | [Add Devices](#) | [Review](#) | [Shipping](#) | [EXIT RETURN](#)

Status of Return

Shipping Label

Retrieve Data
Please retrieve all data, if applicable, from the device prior to returning. We will clear all records before a unit is sent back to you and you may receive a new unit all together. Axon Enterprise, Inc. is not responsible for lost data. Caution: Firing records may be lost or destroyed during the repair process. Unrepairable units are destroyed after analysis, therefore, Axon Enterprise, Inc. strongly recommends that you download the weapon prior to return. If you are unable to download the firing records, please contact customer service at 1-800-978-2737 or 480-905-2000 for further instructions. Additional costs will apply.

Pack Devices
Pack product(s) securely, do not use shredded paper or packing popcorn. Please leave all batteries in place that were present when the problem occurred. Include a copy of this packing slip in each package.

[VIEW PACKING SLIP](#)

[DOWNLOAD](#)

Return Status: Received

- ☒ Shipping Labels Created
- ☒ Shipped To Axon
- ☒ Received by Axon
- ☐ Replacements Ready
- ☐ Shipped by Axon
- ☐ Delivered to Agency

Contact Return

Have a question about your return? Need guidance on proper packing and shipping methods?

[CONTACT RETURN](#)

Return Summary

SUBMISSION	RETURN SUBMITTED	RETURN OWNER
251757	04/16/2019	Dawson Cory

Items in Return (1)

DEVICE TYPE	SERIAL NUMBER	REASON FOR RETURN
Axon Body 2	XB1138209	return

The right side of the page shows the status of the return. Note that the status on this page is derived from FedEx shipping statuses and will be updated periodically throughout the day. If your return did not use the FedEx labels, some steps in the status will be skipped.

If evidence recovery was requested for devices submitted in this return, you to check the status of evidence being recovered without having to contact Axon. This information is shown at the bottom of the page and includes device information, the expected number of videos, the recovery status, and links to any recovered videos. The evidence recovery information is updated twice per day.

From the Status of Return page, you can:

- Click **View Packing Slip** to view and print the packing slip.

This is opened in a new browser tab. A copy of the packing slip should be included in each box. The packing slip also has shipping instructions.

- Click **Download** to download the FedEx shipping labels for printing.
- Click **Contact Return** to start an email message with Axon Returns.
- Click **Exit Return** to go back to the Returns page.

Creating a New Return

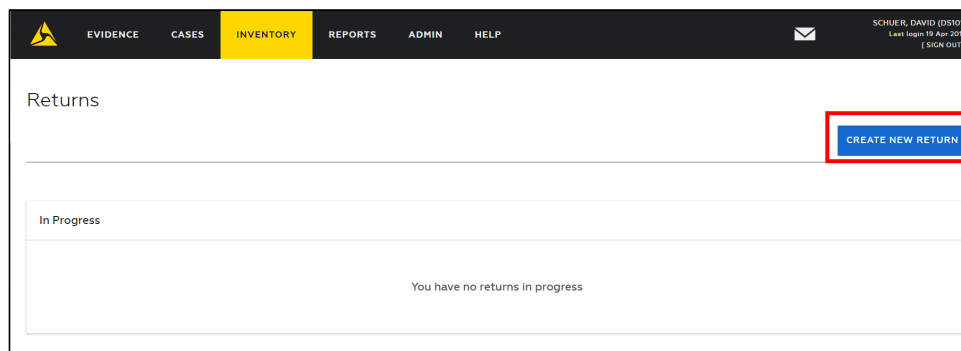
Whenever you need to return devices that are managed in Axon Evidence, you can create a new return.

- For lost/stolen devices, please submit a return for the device, noting the lost/stolen status, and email a copy of any administrative report to RMA@axon.com.
- For devices that are no longer supported, contact your Axon representative to discuss replacement options to meet your agency's needs. If the device requires video recovery, a return can still be submitted for that purpose.

Tip: You can update the status of the devices you are returning before you create the return to make it easier to find the devices (for example change the status to **RMA**). If you change the status, you should leave devices assigned to their current user. See the [Update Device Status article](#) on the Axon Help Center for more information.

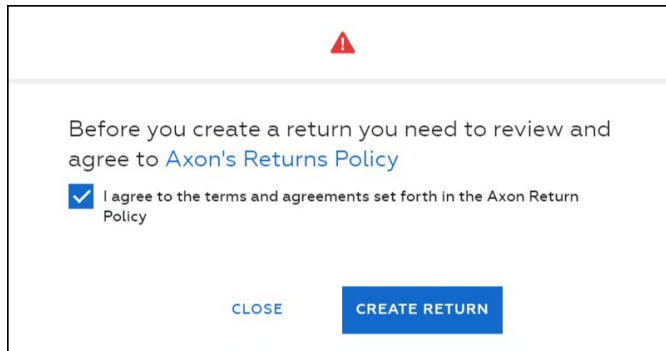
Note: Each user can only have one active in-progress return at a time.

1. On the Returns page, click **Create New Return**, in the upper right.



2. Agree to Axon's Return Policy by selecting the I agree check box and then click **Create Return**.

Click the **Axon's Returns Policy** link to read the policy information.



Before you create a return you need to review and agree to [Axon's Returns Policy](#)

☒ I agree to the terms and agreements set forth in the Axon Return Policy

[CLOSE](#) [CREATE RETURN](#)

3. On the Add Devices by Search page, select the devices you want to return.

Note: You can click **Exit Return**, in the upper right, to save the In-Progress return and go back to the Returns page.

If you are only returning products that do not have a serial number, such as cables and body camera mounts, skip to Step 7.

Use the search filters at the top of the page to narrow the list of devices. You can search by Serial Number, Device Name, Assigned To, Error Status, and Device Status. You don't need to enter information in all of the search fields, just use the ones needed to narrow down the list of devices.

The sort options include Serial Number, Device Name, Last Uploaded, Device Status, Error Status, Firmware Version, and Warranty.

DAVID SCHUER'S RETURN | 1.Add Devices | 2.Review | 3.Shipping | EXIT RETURN

Add devices by Search

SERIAL NUMBER: DEVICE NAME: ASSIGNED TO: ERROR STATUS: DEVICE STATUS:

RESET FILTERS SEARCH

Sort by Warranty Descending Include Added Items

Axon Flex 2 - X83031256 DEVICE STATUS: In Stock ERROR STATUS: Good		DEVICE NAME: X83031256 ASSIGNED TO:	REASON FOR RETURN: Select a Reason EVIDENCE RECOVERY: No THE PRODUCT WAS DROPPED, DAMAGED, OR EXPOSED TO MOISTURE: No	ADDITIONAL INFORMATION: <input type="text"/> ADD
Axon Body 2 - X81240315 DEVICE STATUS: In Stock ERROR STATUS: Good		DEVICE NAME: X81240315 ASSIGNED TO:	REASON FOR RETURN: Select a Reason EVIDENCE RECOVERY: No THE PRODUCT WAS DROPPED, DAMAGED, OR EXPOSED TO MOISTURE: No	ADDITIONAL INFORMATION: <input type="text"/> ADD

REVIEW RETURN ITEMS

4. Once you have located the device you want to return:

- Select a reason for return.
- Select if evidence recovery is needed. This option is not shown for devices that do not record or store evidence.

If **Yes** is selected, select the number of videos for recovery and the Evidence Owner for the recovered evidence. This number is only an estimate. If there are more videos on your device, they will not be discarded.

- Select if the device was dropped, damaged or exposed to moisture.
- Enter any Additional Information or notes about the issues you are experiencing with the device.

5. Click **Add** on the right side of the device to add the device to the In-Progress Return.

Every time a device is added, progress is saved automatically.

- If the device is currently part of another In-Progress Return, a warning message is shown allowing you to override the other In-Progress Return and add the device to your return. You should only use the override option in situations where you physically have the device.

- If the device is part of a Return that has already been submitted, a warning message is shown stating that the device has already been submitted to Axon. Please contact your Axon representative or Technical Support if a device is shown as being part of a return but was not included in the shipment.
6. Repeat steps 4 and 5 for any other devices you want to include in this return.
 7. After all devices have been added, click **Review Return Items** in the lower right corner.

You are taken to the Review Your Return page.

DAVID SCHUER'S RETURN | [Add Devices](#) | **2. Review** | [3. Shipping](#) | [EXIT RETURN](#)

Review Your Return

Overview

2 Devices Total	DEVICE MODEL TASER 7 (1) Axon Body 2 (1)	RETURN OWNER Schueler, David (DS101)
---------------------------	---	--

[ADD ITEM MANUALLY](#) [ADD MORE ITEMS TO RETURN](#)

TASER 7 - X41000215		REASON FOR RETURN *	ADDITIONAL INFORMATION *	
DEVICE STATUS RMA ERROR STATUS Good	DEVICE NAME X4100021 ASSIGNED TO 	REASON FOR RETURN * Switches/Buttons EVIDENCE RECOVERY No THE PRODUCT WAS DROPPED, DAMAGED, OR EXPOSED TO MOISTURE No	<input type="text" value="broken switch"/>	EDIT REMOVE
TASER 7 - X41000215				
Axon Body 2 - X81273482				
DEVICE STATUS Assigned ERROR STATUS Good	DEVICE NAME X81273482 ASSIGNED TO Erik Stevens	REASON FOR RETURN * Docking/Sync EVIDENCE RECOVERY No THE PRODUCT WAS DROPPED, DAMAGED, OR EXPOSED TO MOISTURE No	<input type="text" value="No connection in Dock"/>	EDIT REMOVE

[REVIEW SHIPPING](#)

8. To add items that do not have a serial number:
 - Click Add Item Manually. The Add Item Manually Dialog is shown.

Add Item Manually

PRODUCT NAME *

Specify Product

QUANTITY *

1

☐ The product was dropped, damaged, or exposed to moisture

DETAILED DESCRIPTION OF THE PROBLEM *

CLOSE ADD TO RMA

- Enter the Product Name. For example: Flex 2 cable or body camera mount.
- Enter the number of items of this type that you are returning.
- Select if the product was dropped, damaged or exposed to moisture.
- Enter a detailed description of the problem or notes about the issues you are experiencing with the product.
- Click **Add to RMA**.

The item is added to the returns list.

- Repeat this step to add more items.
9. Review the return information for all the devices.
- Use the **Edit** option on the same line as the device to edit information about the device return.
 - Use the **Remove** option on the same line as the device to remove the device from the return.
 - Click **Add More Items to Returns** to go back to the Add Devices by Search page. This allows you to add more devices to the return.

Once the review is complete, click **Review Shipping** in the lower right.

10. On the Shipping page:

CORY DAWSON | [Add Devices](#) | [Review](#) | 3.Shipping | [EXIT RETURN](#)

Shipping

Your return is almost ready to go.
Confirm your return address and enter your package dimensions to print out pre-paid FedEx shipping labels on your local printer.

AGENCY RETURN ADDRESS
Cory Dawsonb
4254420974
1
sammamish, WA 98075
[Change Address](#)

SHIPPING BOXES

LENGTH (IN)	WIDTH (IN)	HEIGHT (IN)	WEIGHT (LB)
0	0	0	0.00

[ADD ANOTHER BOX](#)

ALTERNATIVE SHIPPING METHODS
Axon uses FedEx for return shipping services. If you want to use your own shipping method, select the option below. You will still be able to print packing slips to place inside the return shipping boxes.

☐ I will use my own shipping method

[SUBMIT RETURN](#)

- Review the Return Address for your agency. The address defaults to the last address used for a return.

If needed, click **Change Address** to change, edit, or add a new return address.

- If you will use the pre-paid FedEx shipping labels, enter the dimensions for each shipping box used with the return.

The system defaults to one shipping box. If you have multiple boxes for the return, click **Add Another Box** and enter the box dimensions.

- If you will not use the pre-paid FedEx shipping labels, under Alternative Shipping Methods, select **I will use my own shipping method**.

You can still print the packing slips associated with the return.

Once you have filled out the shipping information, click **Submit Return**.

11. On the Status of Return page, you can:

251757 | [Add Devices](#) | [Review](#) | [Shipping](#) | [EXIT RETURN](#)

Status of Return

Shipping Label

Retrieve Data
Please retrieve all data, if applicable, from the device prior to returning. We will clear all records before a unit is sent back to you and you may receive a new unit all together. Axon Enterprise, Inc. is not responsible for lost data. Caution: Firing records may be lost or destroyed during the repair process. Unrepairable units are destroyed after analysis, therefore, Axon Enterprise, Inc. strongly recommends that you download the weapon prior to return. If you are unable to download the firing records, please contact customer service at 1-800-978-2737 or 480-905-2000 for further instructions. Additional costs will apply.

Pack Devices
Pack product(s) securely, do not use shredded paper or packing popcorn. Please leave all batteries in place that were present when the problem occurred. Include a copy of this packing slip in each package.

[VIEW PACKING SLIP](#)

[DOWNLOAD](#)

Return Status: Received

- ☒ Shipping Labels Created
- ☐ Shipped To Axon
- ☐ Received by Axon
- ☐ Replacements Ready
- ☐ Shipped by Axon
- ☐ Delivered to Agency

Contact Return

Have a question about your return? Need guidance on proper packing and shipping methods?

[CONTACT RETURN](#)

Return Summary

SUBMISSION	RETURN SUBMITTED	RETURN OWNER
251757	04/16/2019	Dawson Cory

Items in Return (1)

DEVICE TYPE	SERIAL NUMBER	REASON FOR RETURN
Axon Body 2	X81136209	return

- Review information about the return.
- Click **View Packing Slip** to view and print the packing slip.
This is opened in a new browser tab. A copy of the packing slip should be included with each return. The packing slip also has shipping instructions.
- Click **Download** to download the FedEx shipping labels for printing.
- Click **Contact Return** to start an email message with Axon Returns.

12. Click **Exit Return**, in the upper right, to go back to the Returns page.

Canceling a Return

This option allows users to cancel their own device returns. Only returns in the Ready to Ship status can be cancelled and a user cannot cancel a return that was created by another user.

1. On the Returns page, find the return you want to cancel and click **Review**.

2. On the Status of Return page, Click **Cancel Return**.

254649 [Add Devices](#) [Review](#) [Shipping](#) [EXIT RETURN](#)

Status of Return

Shipping Label

Retrieve Data
Please retrieve all data, if applicable, from the device prior to returning. We will clear all records before a unit is sent back to you and you may receive a new unit all together. Axon Enterprise, Inc. is not responsible for lost data.
Caution: Firing records may be lost or destroyed during the repair process. Unrepairable units are destroyed after analysis, therefore, Axon Enterprise, Inc. strongly recommends that you download the weapon prior to return. If you are unable to download the firing records, please contact customer service at 1-800-978-2737 or 480-905-2000 for further instructions. Additional costs will apply.

Pack Devices
Pack product(s) securely, do not use shredded paper or packing popcorn. Please leave all batteries in place that were present when the problem occurred. Include a copy of this packing slip in each package.

[VIEW PACKING SLIP](#)

[DOWNLOAD](#)

Return Status: Submitted

☒ Shipping Labels Created [FEDEX TRACKING](#)

☐ Shipped To Axon

☐ Received by Axon

☐ Replacements Ready

☐ Shipped by Axon

☐ Delivered to Agency

Contact Us

Have a question about your return? Need guidance on proper packing and shipping methods?

[CONTACT US](#)

Cancel Return 254649

Need to cancel a return? Click here to start the process

[CANCEL RETURN](#)

Return Summary

SUBMISSION	RETURN SUBMITTED	RETURN OWNER
254649	07/09/2019	Schueler David

Items in Return (1)

DEVICE TYPE	SERIAL NUMBER	REASON FOR RETURN
TASER 7	X41000409	major error

3. The system provides the option to cancel the current return or to start a new return that includes the devices in the current return.

You have 1 device included in this return. Would you like us to automatically add this device to another ticket?

☐ Yes, save my progress and add the device to a new return.

☒ No, discard my progress.

[CLOSE](#) [CANCEL RETURN](#)

- Saving progress and starting a new return cancels the current return and then allows the user to remove or add items to the new return. After creation, the new return can be submitted normally.
- Discarding progress cancels the current return.

Select the appropriate option and click **Cancel Return**.

Reporting

Axon Evidence allows administrators and those with the reporting permission to generate reports showing Axon Evidence utilization. These options can help your agency turn that data into valuable answers to ensure your Axon Evidence account is providing you with the flexibility and utility your agency deserves.

Axon Evidence reports are csv files 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. The report also includes information on evidence sharing through access control lists for internal and external users and groups, and partner agencies.
- **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.
- **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).
- **User Device History** – Lists Axon CEWs (including TASER 7 Battery, Cartridges, etc.), Axon Body Worn and Flex Cameras, and VieVu Cameras that were assigned to or unassigned from the selected user for the selected date range (Note: Only data from July 2017 to present is available). The report lists the Device Model, Device Name (as shown in Axon Evidence), Serial Number, and Assigned and Unassigned Dates. If the Unassigned Date is blank, the device is still assigned to the user.
- **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.

- **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.
- **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** — Lists all user actions related to sharing evidence and cases. Included in the report are details such as the following examples:
 - Date and time of sharing event
 - Who initiated the sharing event
 - What was shared – evidence or a case
 - How was it shared – internal or external to your Evidence.com agency
 - The ID of the evidence or case shared
 - The recipient of the shared evidence or case
 - The permissions shared to the recipient and how long the link is active
- **Device Summary** – List information on all the devices (body cameras and CEWs) belonging to your agency. The report includes the following information for each device:
 - Device model, name, and serial number
 - Device status
 - First name, last name, and badge ID of assigned user
 - Firmware version
 - Last upload date/time
 - Device last connected Dock (serial number) and date-time for devices that can be placed in Axon Docks.
 - Body Camera Device Settings (Speaker volume, Vibration, Indicator Lights, and Stealth)
 - Error Status
 - Device Home and Point of Contact information

- **User Audit Trail** – Generates the User Audit Trail for a single user, for all users in a Group, or for all users with a selected Rank in a Group. The report includes all the standard user audit trail information and adds columns for Rank and Badge ID.

Note: Users must have the Generate User Audit Trail Report permission enabled for their assigned Role to have access to this report.

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.

REPORT TYPE	RUN DATE	START DATE	END DATE	FILTER	STATUS
User Summary	Dec 3, 2020	Nov 23, 2020	Dec 3, 2020	All Users	Download
Evidence Created	Dec 3, 2020	Nov 22, 2020	Dec 3, 2020		Download

2. Under **Select a Report Type**, click the report that you want to run.
3. Depending on the report type, additional report options appear.
 - If the Select Evidence Group option is shown, do one of the following:
 - Leave the field blank to run the report for all groups.

- To select one Evidence Group begin typing a group name. A list of matching groups is shown as you enter the information. Select the group for the report.
- 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.
- If the Select User report option is shown, begin typing a user name. A list of matching users is shown as you enter the information. Select the user for the report.
- If the Select a Date Range report option is shown and you want to change the date range, do one of the following:
 - If you want to use a standard date range (Yesterday, Last Week, Last 10 Days, Last Month, Year to Date, Last Year), 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.
- If the Filter report options appear, click the grouping option that you want.
- 4. In the report summary on the right side of the page, verify that the report configuration is what you want. If not, modify the report options.
- 5. Click **Run Report**.

The Status column will show when reports are queued for processing, report progress, if the report failed due to an error, and if the report is ready to Download.

When the report is ready, Evidence.com sends you a notification email that includes a download link.

- 6. 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>.

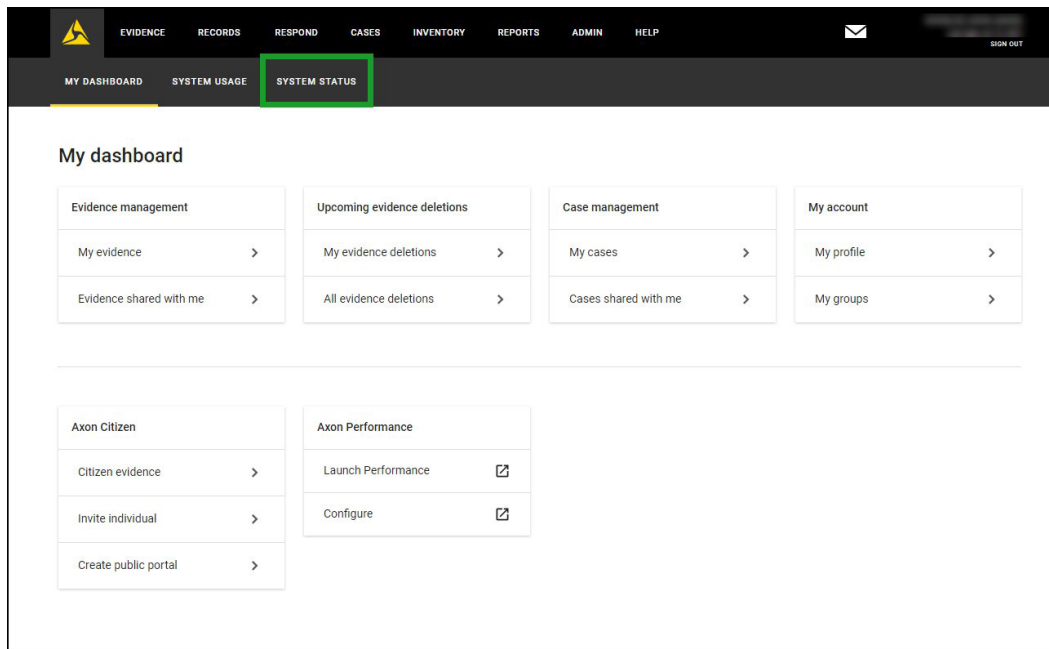
Some examples of what this tool lets you discover:

- 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.

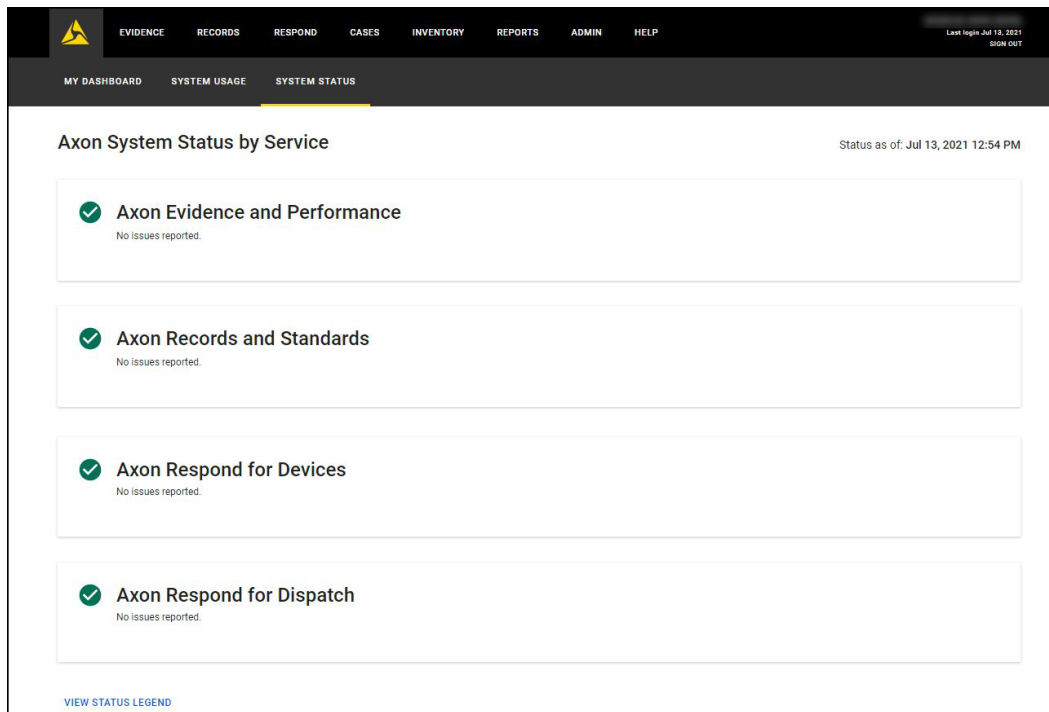
System Status Page

The System Status feature provides a place where authorized users can check the status of Axon cloud service products, such as Axon Evidence. The System Status page is available for customers in the United States, Canada, Australia, New Zealand, and the United Kingdom. It will be available for European customers in a future release.

Authorized users can access the System Status page from their Axon Evidence Dashboard page.



The System Status page shows the current status of Axon cloud services products and includes an area for a short description of any issues.



There are four standard system status, with corresponding icons for quick identification. Each status is described below:

- Operational: Products and services are operational with no service impacts reported.
- Partial Disruption: A partial disruption has been reported on one or more products and services. Status updates will be published as new information becomes available.
- Major Disruption: A major disruption has been reported on one or more products and services. Status updates will be published as new information becomes available.
- Maintenance: We are conducting maintenance on one or more products and services. Updates will be published as the maintenance is conducted.

To see the System Status link on the Dashboard page and access the System Status page, users must be assigned to a role with the System Status - **View Status Page permission** set to Allowed. This permission is set to allowed by default for the pre-configured Admin role.

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 Axon Evidence user account can have one of the following possible statuses.

- **Active** — The user can access your Axon Evidence agency, as determined by the role that you assigned to the user account. Administrators can change user account information for Active users.

Axon Evidence 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 Axon Evidence 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 Axon Evidence 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.

Users

66 results

ADD USER

IMPORT USERS

EXPORT RESULTS

...

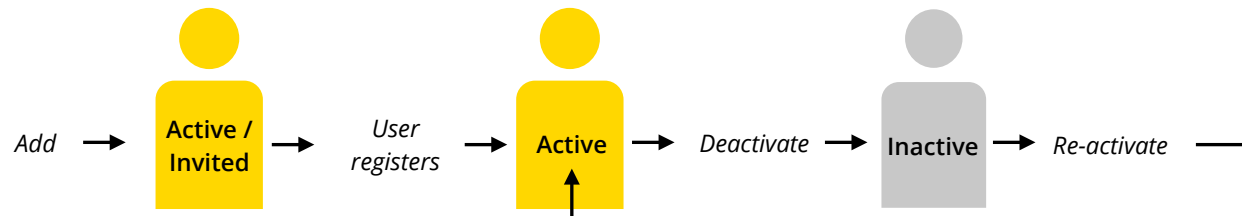
<input type="checkbox"/>	Name	Badge ID	Role	Tier	Last active ↑	Invited date	Deactivated date	Status
<input type="checkbox"/>	Gray, William	040620	Admin	Pro	Jun 2, 2021 4:49 AM	Apr 16, 2020 7:05 AM		Active
<input type="checkbox"/>	Carter, Keith	5899	User	Basic		May 4, 2020 5:26 PM		Invited
<input type="checkbox"/>	User, Jenny	1245	User	Basic	May 18, 2016 11:41 ...	May 18, 2016 11:29 A...		Password Reset
<input type="checkbox"/>	Jones, John					Apr 15, 2013 1:29 PM		Inactive

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.

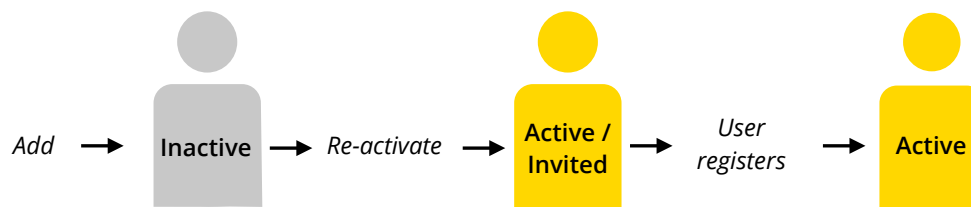
User Account Added as Active

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.



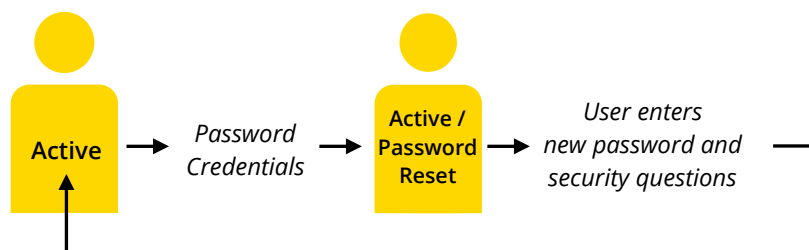
User Account Added as Inactive

The following figure shows the progression of states from Inactive to Active when a user is added in the Inactive state.



Active User Account During Password Reset

The following figure shows the progression of states between Active and Active/Password Reset.



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 click **All Users**. On the Users page click **Add User**.

The Add User page appears.

2. In the following fields, type the information.
 - **First Name** (Required) — The user's first name.
 - **Last Name** (Required) — The user's last name.
 - **Rank** (Optional) — Select the appropriate Rank for the user.
 - **Evidence Group** (Optional) — Select the appropriate Evidence Group for the user. See [Evidence Groups](#) for more information.
 - **Badge ID** (Required) — 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.
 - **Direct Supervisor** (Optional) – Select the user's direct supervisor.
 - **Username** (Required) — A unique username that you assign.
 - **Email Address** (Required) — The unique Internet email address of the user.
 - **External ID** (Optional) — 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.
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 or edit many users to your Evidence.com agency, use the Import Users feature. This feature lets you create or edit many user accounts quickly. You specify details about the users in a Comma-separated values (CSV) file that you upload to Evidence.com.

The Import Users feature provides two import options:

- The **Add or update user accounts** option is used to add new users to Axon Evidence and update existing users based on the information in the CSV file. Any user accounts that are not explicitly referenced in the CSV file will not be affected.
- The **Synchronize all user accounts** option affects all active user accounts, regardless of whether the user account is explicitly referenced in the CSV file. Users that have a status of Active that are not included the CSV file have their status changed to Inactive. This option is useful when you want to use the contents of the CSV file as a definitive list of all Active user accounts.

The CSV file for importing users must contain a header row and must have eight columns. When updating users, if an optional column is not included in the CSV, the import will make no changes to those attributes of a user. If optional columns are included, the import process uses the values provided in the column for each user. For example, if the CSV file includes the rank column and the value is empty for a specific user, the user's rank will be

removed. The following table describes the required and optional values in the CSV file for importing users:

Header Value	Value
EXTERNAL_ID	<p>REQUIRED</p> <p>A unique value that identifies the user. The external ID is assigned by your organization. It is recommended that you determine a user ID strategy that best suits your needs.</p> <p>Note: The external user ID is an immutable value. After a user account is created, you cannot change its external ID. If you try to change the external ID of an existing user account, Evidence.com interprets the new external ID as a new user and attempts to create a new user account.</p> <p>If you are synchronizing the users in your Evidence.com agency with users in another application, you may want to use an ID value provided by the other application, such as a GUID.</p> <p>You can also simply assign a descriptive name.</p> <p>If a user account was created through the Evidence.com web user interface, the external user ID is a GUID assigned by Evidence.com and is included in the response to any user-related request.</p> <p>Valid external user IDs can be up to 255 characters.</p> <p>Note: You can use the Export Results option on the All Users search page to export user information that includes the External ID for users.</p>
EMAIL	<p>REQUIRED</p> <p>The Internet email address of the user. Each user in your agency must have a unique email address.</p>
BADGE_NUMBER	<p>REQUIRED</p> <p>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.</p> <p>Note: If your organization does not assign badge numbers to users, it is recommended that you put user email addresses in the BADGE_NUMBER column, too.</p>
FIRST_NAME	<p>REQUIRED</p> <p>The user's first name.</p>
LAST_NAME	<p>REQUIRED</p> <p>The user's last name.</p>
STATUS	<p>REQUIRED</p> <ul style="list-style-type: none"> • Active — The user is able to register and sign in to Evidence.com immediately after you import the user account. • Inactive — The user is not able to register or sign in to Evidence.com.

Header Value	Value
USERNAME	REQUIRED A unique username.
ROLE	REQUIRED The role that you want to assign to the user. Valid values are the names of the roles configured in your Evidence.com agency.
SUPERVISOR_EMAIL	OPTIONAL The user's direct supervisor. If included, the supervisor's email address, as used in Axon Evidence, should be entered in the field.
LOCATION	OPTIONAL Reserved for future use.
RANK	OPTIONAL The rank that you want to assign to the user. Valid values are the names of the ranks configured in your Evidence.com agency.
EVIDENCE_GROUP_EXT_ID	OPTIONAL The External_ID of the group to be assigned to the user. Must be an active group.
PHONE	OPTIONAL Phone number in the format + country code phone number. Example: +15105551212. Note: If you are using Microsoft Excel to create the CSV file, verify the + is not removed when the file is saved.

To import users into your account:

1. On the menu bar, click **Admin** and then click **All Users**. On the Users page click **Import Users**.
2. Download the example file.
3. Make a copy of the example file and assign it a meaningful file name.
4. Open the file in the appropriate application using a spreadsheet application.

The first row or line of the file contains column names. The second through fifth rows are examples.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	EXTERNAL_ID	EMAIL	BADGE_NUMBER	FIRST_NAME	LAST_NAME	STATUS	USERNAME	ROLE	SUPERVISOR_EMAIL	LOCATION	RANK	EVIDENCE_GROUP_EXT_ID	PHONE
2	API1	user1@example.com	BID001	First1	Last1	Active	user1@example.com	Admin	supervisor1@example.com	Seattle	Sergeant	SDA6D9F3-38C9-4EFD-8A0C	15105551212
3	API2	user2@example.com	BID002	First2	Last4	Active	user2@example.com	User	supervisor1@example.com	Seattle			
4	API3	user3@example.com	BID003	First3	Last4	Inactive	user3@example.com	User	supervisor1@example.com	Seattle	Officer	GROUP_5447	
5	API4	user4@example.com	BID004	First4	Last4	Inactive	user4@example.com	Investigator	supervisor1@example.com	Seattle	Officer		

5. Delete the information in the second through fifth lines. *Do not* delete the first line. Evidence.com expects the first line to contain the column names.
6. Enter the user information in the file. The information entered depends on if you are only adding or modifying user accounts or if you are synchronizing all user accounts.

- If you are adding or modifying user accounts, for every user that you want to add or edit include a line in the file that specifies values for the user. When editing a user account, enter the new value in the appropriate column.

Example: If you are changing a user from active to inactive, you would enter Inactive in the Status column for the user.

- If you are synchronizing all user accounts, you must include all active user in the file. Even if there are no changes to the user's information. Users that have a status of Active that are not included the CSV file have their status changed to Inactive.
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. Select the **Import Option** you want to use (Add or update user accounts or Synchronize all user accounts).
 10. Click **Select File** and, in the dialog box that opens, select the file on your computer, and then click **Open**.
 11. Click **Upload**.

Evidence.com imports the file. When the upload is complete, a summary of import is displayed showing which users were added, updated, and where there are errors.

You can upload another file or navigate to another action.

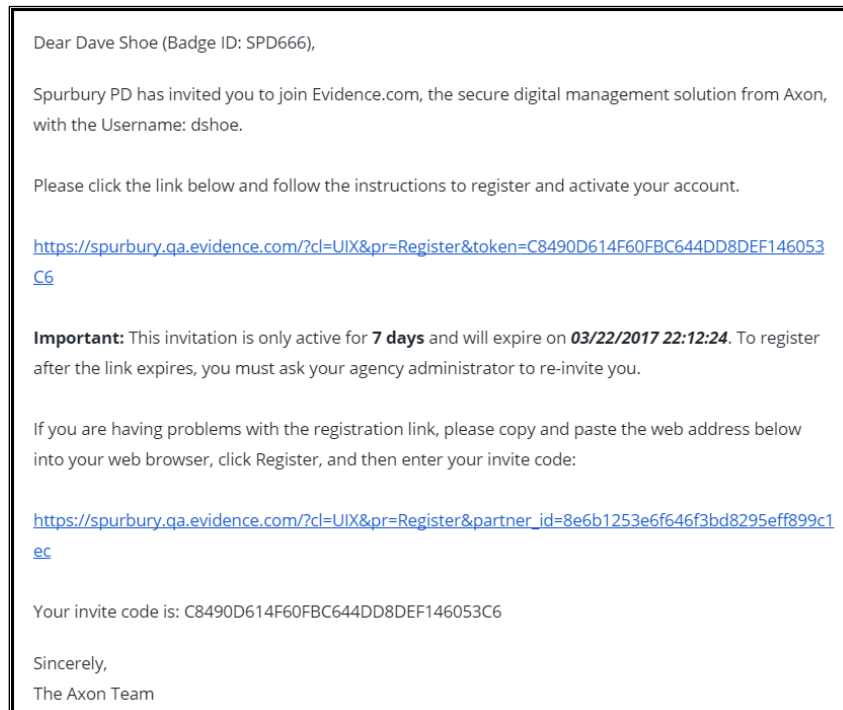
Complete the User Registration Process

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.



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.

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 Detail page.

Deactivate Many Users

From a user search page, you can deactivate more than one user account at a time.

Note: You can also use the Import User function to change the status of multiple users by changing the user Status in the upload file.

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. Use the user search filters to refine the search results.

For example, to search for all active users, click Show Advanced Search, set the **Status** filter to **Active**, and then click **Search**.

Use additional search filters as needed to refine the search results.

3. 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.

4. Click **Deactivate** or click the ... (more actions) menu and select **Deactivate**.

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.

5. If you do *not* want to reassign the users' evidence and devices, skip to step 9.
6. If you want to reassign the users' evidence and devices, click **Reassign the Evidence and Devices to Another User**.
7. 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.

8. Click the user to whom you want to reassign evidence and devices.
9. Click **Deactivate User**.
10. 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.

11. If you want to confirm that the accounts are deactivated, search for the users again.

Deactivate One User

You can deactivate a single user from the User Detail 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 active user whose account you want to deactivate.
3. In the user search results, click the user name.

The User Detail page appears.

4. Click the ... (More Actions) menu and select **Deactivate user**.
5. A Deactivate User panel is shown on the right side of the page and you are asked to choose a user that evidence files and devices will be assigned to when the current user is deactivated.
 - If you do *not* want to reassign the user's evidence and devices, select the **Still assigned to <username>** option and click **Deactivate**.
 - If you want to reassign the user's evidence and devices, select **Reassigned to another user**.

In the **Reassign to** field, 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.

Select the user to whom you want to reassign evidence and devices.

Click **Deactivate and Reassign**.

6. A notification message appears at the top of the page stating that the user account has been deactivated and, if selected, that items were reassigned.

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 users in two ways:

- Many users at once, from user-search results.
- One user at a time, from a User Summary page.

Reactivate Many Users

From the User Search page, you can reactivate user accounts that have a status of Inactive.

Note: You can also use the Import User function to change the status of multiple users by changing the user Status in the upload file.

1. On the menu bar, click **Admin** and then under Users, click **All Users**.
2. Use the user search filters to refine the search results.

For example, to search for all inactive users, click Show Advanced Search, set the **Status** filter to **Inactive**, and then click **Search**.

Use additional search filters as needed to refine the search results.

3. 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.
4. Click **Reactivate** or click the ... (more actions) menu and select **Reactivate**.
5. On the confirmation message box, click **OK**.
6. 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.

7. If you want to confirm that the accounts are active, search for the users again.

Reactivate One User

You can reactivate a single user from the User Detail 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 active user whose account you want to reactivate.
3. In the user search results, click the user name.

The User Detail page appears.

4. Click **Reactivate**.
5. You are asked to confirm the reactivation. Click **Reactivate** to continue.
6. A notification message appears at the top of the page stating that the user account has been reactivated.

Evidence.com sends a notification email to the user whose account you reactivated.

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.

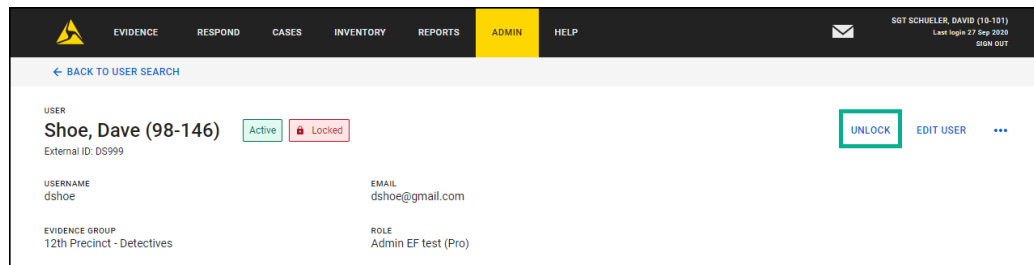
2. Search for the user whose account you want to unlock.

User search results do *not* show whether an account is locked.

3. In the user search results, click the user name.

The User Detail page appears.

4. Click **Unlock**.



5. The system confirms the account is unlocked.

The user account is unlocked, the page refreshes, and the Unlock option is no longer 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 Detail page appears.

4. Click the ... (More Actions) menu and select **Reset credentials**.
5. You are asked to confirm the action, click **Reset Credentials**.

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 the ... (more actions) menu and select **Reset Credentials**.
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.

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 Detail page appears.

4. Click **Edit User**.

5. In the Edit User information panel, 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, rank, evidence group, 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 Detail page appears.

4. Click **Edit User**.

5. In the Edit User Information panel, update the user information 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.

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 Detail page appears.

4. Click the ... (More Actions) menu and select **View audit trail**.

A dialog box provides options for the date range and file type.

5. Under **Date Range**, select the portion of the audit trail you want to view.

If you select Custom Date Range, you are asked to specify a start and end date.

6. Under **Select File Type**, click the file type (PDF or CSV) that you want.
7. Click **Download**.

Evidence.com downloads the user audit trail in the format you selected. 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 Expire Passwords for all users, click **Expire Passwords**.
3. On the confirmation dialog box, click **Continue**.

The next time each user signs in to your agency, they are required to change their password.

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.

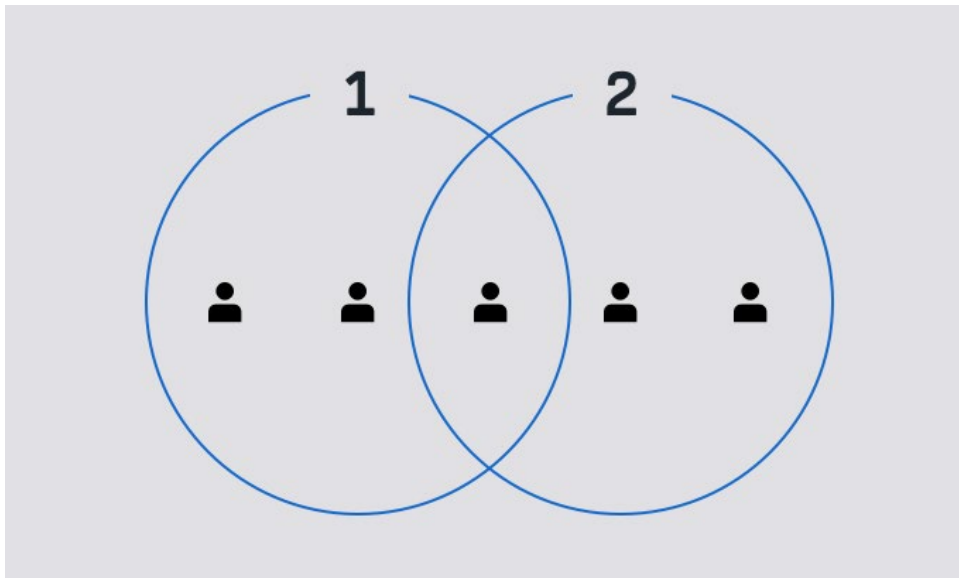
The Groups feature complements the Roles and Permissions feature. Unit leaders no longer must be granted permission to view all evidence of your agency, and you should remove this permission from leaders when you implement the Groups feature.

This section describes the Groups feature, the use of groups for evidence monitoring, and the group-related tasks that you can perform.

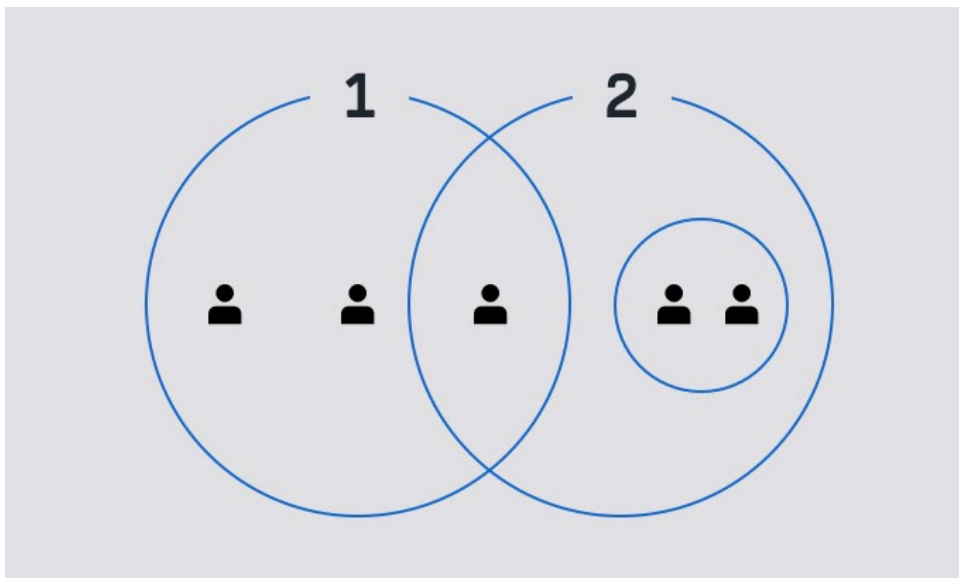
Groups and Membership

Each group that you create has a name, one or more members, and 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.

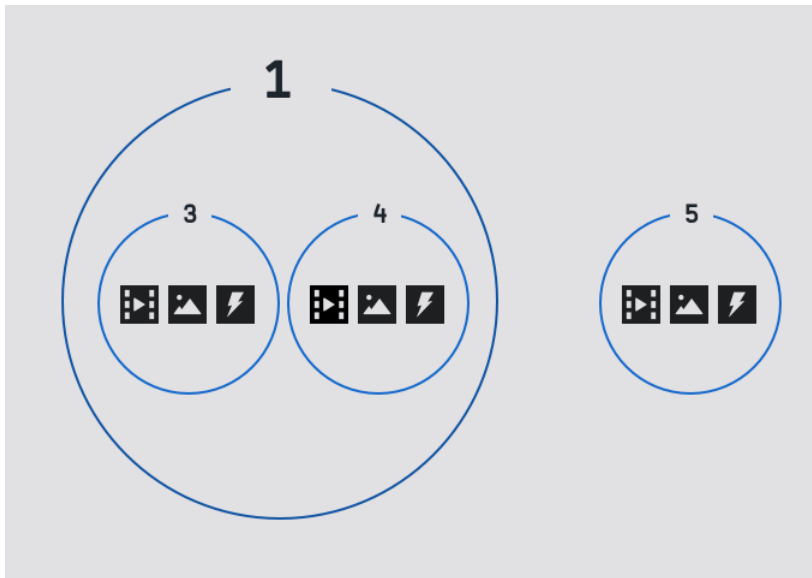
Monitoring Evidence with Groups

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.

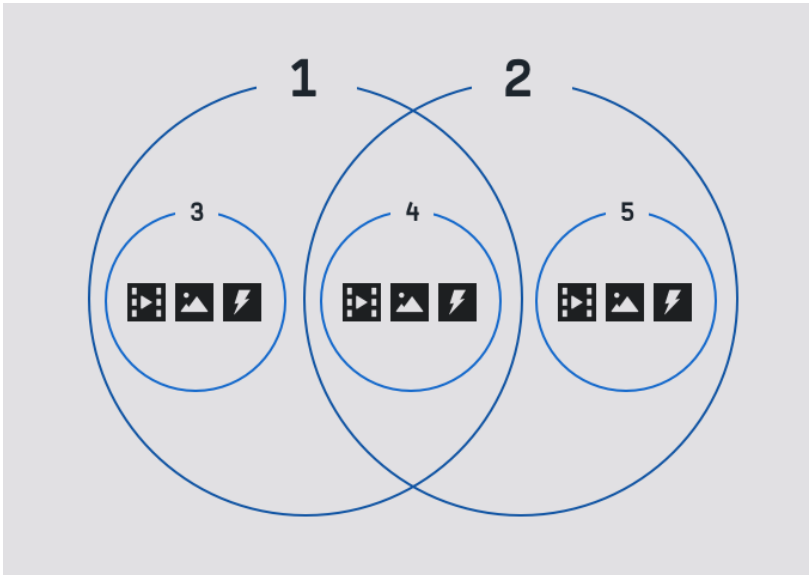


Note: In the preceding example, users who do not monitor group 5 evidence but who are allowed the User Search permission can see group 5 evidence listed in evidence search results but cannot view the evidence without first requesting access.

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 **All Groups**. On the Groups page click **Create Group**. The Create Group page appears.

The screenshot shows the 'Create a new group' form in the Axon Evidence interface. The form is titled 'Create a new group' and is part of the 'ADMIN' section. It includes the following fields and options:

- GROUP NAME**: A text input field.
- ACCESS SETTINGS**: Three radio button options:
 - No access**: This group cannot be added to access lists.
 - Inside my agency access**: This group can be added to access lists inside my agency. Monitors can view evidence owned by group members.
 - Partner agency access**: This group can be added to access lists inside and outside my agency. Monitors can view evidence owned by group members.
- ENABLE COACHING**: A checkbox for **Coaching Specialty Group**. This group can be added as a Coaching Specialty Group. Other officers can make a coaching request from group members.
- EXTERNAL ID**: A text input field. When left empty, external ID will be automatically generated.
- Create another right after**: A checkbox.
- CANCEL** and **CREATE** buttons at the bottom.

2. Name the Group and set the Access Setting

The group name must be at least three characters long and can be a maximum of 128 characters long.

There are three 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 Access Setting, Group Monitors can view evidence owned by Group Members.

3. If this group is being set up as a Coaching Group, select **Coaching Specialty Group**.

4. Optionally, enter an **External ID** for the group.

This is a unique value that identifies the group. If you do not enter a value, an External ID is automatically generated by the system.

This ID is persistent and unchanging for the life of the group. If the ID is assigned by your organization. It is recommended that you determine a group ID strategy that best suits your needs.

To find the external group ID for an existing group, view the Group Profile page for the group.

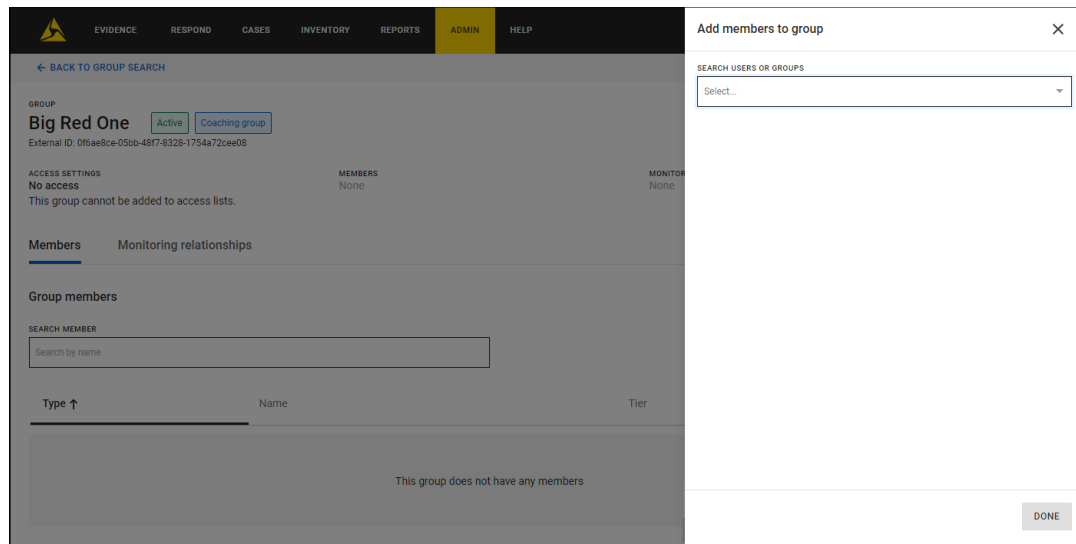
5. If you want to create additional Groups without adding members, select **Create another right away**.

6. Click **Create**.

If you selected to create another group right away, the group information is saved and a new Create Group page is shown. Repeat steps 2 – 6 to create the new group.

7. On the group page, click **Add Members**.

8. For each user or group that you want to add as a group member, in the **Search Users or Groups** box, start typing the name of the user or group, wait for Evidence.com to show the list of matching users or groups, and then click the name of user or group that you want add.



When all group members have been added, click **Done**.

9. Optionally, click the **Monitoring relationships** tab to add group monitors. 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 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:

- **Group monitors:** This sets the users and groups that can access evidence owned by members of this group.
- **Monitored by this group:** 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 10.

Otherwise, once you have decided which type of Monitoring Relationship to use:

- Click **Add Monitors** to add group monitors. For each user or group that you want to add as a monitor, in the **Search Users or Groups** box, start typing the name of the user or group, wait for Evidence.com to show the list of matching users or groups, and then click the name of user or group that you want add.
- Click **Add Groups** to add groups to monitor. For each group that you want this group to monitor, in the **Search Groups** box, start typing the name of the group, wait for Evidence.com to show the list of matching groups, and then click the name of group.

When all monitoring relationships have been added, click **Done**.

10. Click **Back to Group Search** or navigate to any other page.

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:

Column	Header Value	Value
A	EXTERNAL_ID	<p>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.</p> <p>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.</p> <p>To find the external group ID for an existing group, view the Group Profile page for the group.</p> <p>You can also simply assign a descriptive name.</p> <p>Valid external group IDs can be up to 255 characters.</p>
B	NAME	<p>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.</p> <p>Valid group titles can be up to 128 characters.</p>
C	SHARE_ACCESS	<p>Sets the access levels for the group and corresponds to the Manage Access Settings. Valid values are the following three words:</p> <ul style="list-style-type: none"> • 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 **All Groups**. On the Groups page click **Import Groups**.
3. With the Import Option set to Create groups or Synchronize groups, click **Download Example File** to save the example csv file 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.

	A	B	C
1	EXTERNAL_ID	NAME	SHARE_ACCESS
2	EXT_1	IMPORT GROUP 1	FORBIDDEN
3	EXT_2	IMPORT GROUP 2	INTERNAL
4	EXT_3	IMPORT GROUP 3	ANY

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. Return to the Import Groups page in Evidence.com.
10. Select the appropriate Import Option for the action you want to complete.
 - Select **Create groups** if you want to add the groups in the CSV file without affecting any existing groups.
 - Select **Synchronize groups** if you want to *completely replace all groups currently in your agency* with the groups in your groups CSV file,
11. Under Upload file, click **Select File** and, in the dialog box that opens, select the groups CSV file on your computer, and then click **Open**. Then click **Upload**.

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.

12. Review the list of actions taken.
13. If you need to correct errors, update the groups CSV file as needed, click **Import Another File**, and repeat this procedure.
14. 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:

Column	Header Value	Value
A	EXTERNAL_ID	<p>External group ID — The ID of the group to which the member or monitor is added.</p> <p>This ID must match the external group ID used to create the group. For more information, see Import Groups.</p> <p>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.</p> <p>Valid external group IDs can be up to 255 characters.</p>
B	MEMBERSHIP_TYPE	<p>Member or monitor — Whether the row in the CSV file defines a member or a monitor.</p> <p>Valid values are the following two words:</p> <ul style="list-style-type: none"> • MEMBER • MONITOR <p>The valid values are case insensitive.</p>
C	ENTITY_TYPE	<p>User or group — Whether the member or monitor is a user or a group.</p> <p>Valid values are the following two words:</p> <ul style="list-style-type: none"> • USER • GROUP <p>The valid values are case insensitive.</p>
D	ENTITY_ID	<p>Identifier of the member or monitor.</p> <ul style="list-style-type: none"> • 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.

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 **All Groups**. On the Groups page click **Import Groups**.

3. With the Import Option set to Add members and monitors or Synchronize members and monitors, click **Download Example File** to save the example csv file to your computer.

Import groups

IMPORT OPTION
Add members and monitors

This option adds members and monitors to groups, as specified in the CSV file, without altering the group members and monitors already configured in your agency.

Groups are identified by external ID and users are identified by email address.

[DOWNLOAD EXAMPLE FILE](#)

Upload file
Accepted file type is comma separated value (.csv).

[SELECT FILE](#)

[UPLOAD](#)

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.

	A	B	C	D
1	EXTERNAL_ID	MEMBERSHIP_TYPE	ENTITY_TYPE	ENTITY_ID
2	EXT_1	member	user	user@evidence.com
3	EXT_1	monitor	user	user2@evidence.com
4	EXT_2	member	group	EXT_3
5	EXT_3	monitor	group	EXT_2

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. Return to the Import Groups page in Evidence.com.
10. Select the appropriate Import Option for the action you want to complete.
 - Select **Add members and monitors** if you want to add the groups in the CSV file without altering any existing group members and monitors.

- Select **Synchronize members and monitors** if you want to *add new members or monitors and remove any members or monitors that are not specified in the CSV file*.
11. Under Upload file, click **Select File** and, in the dialog box that opens, select the member and monitor CSV file on your computer, and then click **Open**. Then click **Upload**.

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.
 12. Review the list of actions taken.
 13. If you need to correct errors, update the CSV file as needed, click **Import Another File**, and repeat this procedure.
 14. 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

The My Groups section of 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 profile page, see [Viewing My Groups 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 detail 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. On the menu bar, click **Admin** and then under Users, click **All Groups**. On the Groups page 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.

Task	Steps
Change the group name	<ol style="list-style-type: none"> 1. Click Edit Group. 2. Type the new name. 3. Click Save.
Change the group Access Setting	<ol style="list-style-type: none"> 1. Click Edit Group. 2. Select the appropriate Access Setting for the group. 3. Click Save.
Add a user or group to the group members list.	<ol style="list-style-type: none"> 1. Click Add Member. 2. Start typing the name of the user or group. 3. Wait for Evidence.com to show the list of matching users and groups. 4. Click the user or group you want to add. 5. After all users and groups have been added, click Done.
Delete a user or group from the group members list.	<ol style="list-style-type: none"> 1. In the group member list find the user or group. 2. To the right of the user or group name click the Remove from group icon.
Add a user or group to the monitoring relationship list.	<ol style="list-style-type: none"> 1. Click the Monitoring relationships tab. 2. Click Add Monitors or Add Groups. 3. Start typing the name of the user or group. 4. Wait for Evidence.com to show the list of matching users and groups. 5. Click the user or group you want to add. 6. After all monitoring relationships have been added, click Done.
Delete a user or group from the monitoring relationship list.	<ol style="list-style-type: none"> 1. Click the Monitoring relationships tab. 2. In the group monitors or monitored by this group list find the user or group. 3. To the right of the user or group name click the Remove from group icon.

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. On the menu bar, click **Admin** and then under Users, click **All Groups**. On the Groups page, search for the group for which you need to view evidence.

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. On the menu bar, click **Admin** and then under Users, click **All Groups**. On the Groups page, search for the group for which you need to view the audit trail.

2. In the group search results, click the group title.

The Group Profile page appears.

3. Click ... (More Actions) and select **View audit trail**.

A dialog box provides options for viewing the entire audit trail or a portion of the audit trail.

4. Click **Download**.

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.


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. On the menu bar, click **Admin** and then under Users, click **All Groups**. On the Groups page, search for the group you want to delete.
2. In the group search results, to the left of the group title, click  (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 ... (More Actions) and select **Delete Group**.
4. On the confirmation message box, click **Delete Group**.

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.

Evidence Groups

Evidence Groups build on-top of the existing Group feature in Axon Evidence.com to enable agencies to automatically assign evidence ownership to a Group and automate evidence access based on group membership. While users can be members/monitors of multiple groups at one time, each user and each piece of evidence can only be assigned to one Evidence Group at one time.

Evidence Groups are not a new resource in Axon Evidence.com. Every existing Group can use the Evidence Group functionality. Each piece of evidence will still have a Recorded By attribute, which must be populated with a User, but will now also have an associated Evidence Group attribute.

The primary difference between a Group and an Evidence Group is how they enable access to evidence. Group Monitors can access all evidence owned by Group Members, as long as the user that recorded the evidence is still a member of the group. Evidence Groups allows evidence to be assigned to the group and for users with the appropriate permissions to be able to access that evidence. This ensures users with the appropriate permissions can always access all evidence assigned to their groups; even if the user that recorded the evidence is no longer a member of the group.

Using Evidence Groups

When planning to use Evidence Groups, an agency should follow the same guidelines and considerations as when [implementing other Groups](#) with the following additions:

- Review policies and requirements for evidence access for your agency's groups.
- Review your roles and permissions to determine if any changes are needed to the Evidence Management permissions. Create or update the roles and permissions as needed and then assign users to the appropriate roles.
- Assign users to Evidence Groups as needed. Every user can optionally have one Group assigned as their Evidence Group. All evidence recorded by the user is automatically assigned to the user's Evidence Group upon ingestion into Axon Evidence.com.

- Evidence can be manually assigned to an Evidence Group, but Axon recommends that agencies using Evidence Groups assign users that can upload evidence to an Evidence Group to automate evidence assignment and access.

Example Evidence Group Setup and Scenarios

This section provides an example setup and use of Evidence Group functionality.

Example Role Permissions

In this example, the agency has set up three Roles – Patrol Officer, Detective, and Supervisor. For the example, we are interested in the Evidence Management permissions for the Roles.

Role Name: Patrol Officer

- Evidence Management – View and Edit permissions = Only their own

Role Name: Detective

- Evidence Management - View and Edit permissions = Their groups' & their own

Role Name: Supervisor

- Evidence Management – View and Edit permissions = Their groups' & their own
- Evidence Management – Edit Evidence Group permission = Their groups' & their own

Example User Role and Evidence Group Assignments

In this example there are three users, and each is assigned to a different Role and Evidence Group.

- **User 1:** Role = Patrol Officer and Evidence Group = 5th Precinct Patrol
- **User 2:** Role = Detective and Evidence Group = Homicide Investigations
- **User 3:** Role = Supervisor and this user is not assigned to an Evidence Group.

Example Group Membership

In this example, there are two groups with the following membership:

Group: 5th Precinct Patrol

Members: User 3

Group: Homicide Investigations

Members: User 2 and User 3

Evidence Access

Based on the example setup, the following evidence access conditions would exist:

User 3 (Supervisor)

- User 3 has access to all evidence whose evidence group is either 5th Precinct Patrol or Homicide Investigations. This is because User 3's role grants them access to their groups' evidence and User 3 is a member of both the 5th precinct Patrol and Homicide Investigations groups.
- User 3 automatically gains access to all evidence uploaded by User 1 and User 2. This is because User 1's Evidence Group is 5th Precinct Patrol and User 2's Evidence Group is Homicide Investigations. As such, all evidence uploaded by User 1 will automatically have its Evidence Group set to 5th Precinct Patrol and all evidence uploaded by User 2 will automatically have its Evidence Group set to Homicide Investigations. User 3's role grants them access to their groups' evidence and User 3 is a member of both the 5th precinct Patrol and Homicide Investigations groups.
- User 3 can change the Evidence Group for a piece of evidence, because User 3's role grants them permission to edit the Evidence Group for their groups' evidence.

User 2 (Detective)

- When User 2 uploads evidence the evidence's evidence group will be set to Homicide Investigations, because User 2's Evidence Group is Homicide Investigations.
- User 2 has access to all evidence whose evidence group is Homicide Investigations, because User 2's role grants them access to their groups' evidence and User 2 is a member of the Homicide Investigations group.
- User 2 has access to evidence they recorded and evidence with the Homicide Investigations evidence group. This is because User 2 recorded the evidence and their role allows them to view their own evidence. User 2 also has access to this evidence because their role grants them access to their groups' evidence and User 2 is a member of the Homicide Investigations group.
- User 3 also has access to evidence uploaded by User 2, because User 3 is a member of the Homicide Investigations Group and their role allows them to access their groups' evidence.

User 1 (Patrol Officer)

- When User 1 uploads evidence the evidence's evidence group will be set to 5th Precinct Patrol, because User 1's Evidence Group is 5th Precinct Patrol.
- User 1 has access to the evidence they uploaded, because User 1 recorded the evidence and their role allows them to view their own evidence.
- User 3 also has access to the evidence uploaded by User 1, because User 3 is a member of the 5th Precinct Patrol Group and their role allows them to access their groups' evidence.

Permissions and Evidence Groups

Evidence Group functionality is directly related to the following Evidence Management permission and settings.

Evidence Management				
View	<input type="radio"/> ANY EVIDENCE	<input checked="" type="radio"/> THEIR GROUPS' & THEIR OWN	<input checked="" type="radio"/> ONLY THEIR OWN	<input type="radio"/> PROHIBITED
View CEW Firing Logs	<input type="radio"/> ANY EVIDENCE	<input checked="" type="radio"/> THEIR GROUPS' & THEIR OWN	<input type="radio"/> ONLY THEIR OWN	<input type="radio"/> PROHIBITED
Edit	<input type="radio"/> ANY EVIDENCE	<input checked="" type="radio"/> THEIR GROUPS' & THEIR OWN	<input type="radio"/> ONLY THEIR OWN	<input type="radio"/> PROHIBITED
Add/Remove Pending Review Category	<input type="radio"/> ANY EVIDENCE	<input checked="" type="radio"/> THEIR GROUPS' & THEIR OWN	<input type="radio"/> ONLY THEIR OWN	<input type="radio"/> PROHIBITED
Edit Evidence Group 1	<input type="radio"/> ANY EVIDENCE	<input checked="" type="radio"/> THEIR GROUPS' & THEIR OWN	<input type="radio"/> ONLY THEIR OWN	<input type="radio"/> PROHIBITED
Redact Pro	<input type="radio"/> ANY EVIDENCE	<input checked="" type="radio"/> THEIR GROUPS' & THEIR OWN	<input type="radio"/> ONLY THEIR OWN	<input type="radio"/> PROHIBITED
Order Transcript Pro			<input type="radio"/> ALLOWED	<input checked="" type="radio"/> PROHIBITED
Reassign	<input type="radio"/> ANY EVIDENCE	<input checked="" type="radio"/> THEIR GROUPS' & THEIR OWN	<input type="radio"/> ONLY THEIR OWN	<input type="radio"/> PROHIBITED
Delete Evidence & Edit Date Recorded	<input type="radio"/> ANY EVIDENCE	<input checked="" type="radio"/> THEIR GROUPS' & THEIR OWN	<input type="radio"/> ONLY THEIR OWN	<input type="radio"/> PROHIBITED
Download	<input type="radio"/> ANY EVIDENCE	<input checked="" type="radio"/> THEIR GROUPS' & THEIR OWN	<input type="radio"/> ONLY THEIR OWN	<input type="radio"/> PROHIBITED
Download Infected Files			<input type="radio"/> ALLOWED	<input checked="" type="radio"/> PROHIBITED
Share	<input type="radio"/> ANY EVIDENCE	<input checked="" type="radio"/> THEIR GROUPS' & THEIR OWN	<input type="radio"/> ONLY THEIR OWN	<input type="radio"/> PROHIBITED
Restrict	<input type="radio"/> ANY EVIDENCE	<input checked="" type="radio"/> THEIR GROUPS' & THEIR OWN	<input type="radio"/> ONLY THEIR OWN	<input type="radio"/> PROHIBITED
Share Externally to Authenticated Users			<input type="radio"/> ALLOWED	<input checked="" type="radio"/> PROHIBITED
Share External Download Links			<input type="radio"/> ALLOWED	<input checked="" type="radio"/> PROHIBITED
Post Notes	<input type="radio"/> ANY EVIDENCE	<input checked="" type="radio"/> THEIR GROUPS' & THEIR OWN	<input type="radio"/> ONLY THEIR OWN	<input type="radio"/> PROHIBITED
Audit Trail PDF	<input type="radio"/> ANY EVIDENCE	<input checked="" type="radio"/> THEIR GROUPS' & THEIR OWN	<input type="radio"/> ONLY THEIR OWN	<input type="radio"/> PROHIBITED
Access Restricted Evidence Pro			<input type="radio"/> ALLOWED	<input checked="" type="radio"/> PROHIBITED

1: Edit Evidence Group Permission

- This permission allows a user to modify the evidence group for a piece of Evidence. This permission is unlocked by the Evidence Management **Edit** permission. By default, this permission is set to Any Evidence for the pre-configured Admin Role. All other pre-configured Roles are set to Prohibited.

2: Their Groups' & Their Own Setting

- This setting allows users assigned to conduct the associated permission actions on their own evidence and all evidence assigned to any group the user is a member or monitor of.

Assigning Users to Evidence Groups

Every user can optionally have one Group assigned as their Evidence Group. All evidence recorded by the user is automatically assigned to the user's Evidence Group upon ingestion into Axon Evidence.com.

User Evidence Group information is included in the User Summary report. This report can be filtered to only show users from a selected Evidence Group.

Users assigned to Roles with the User Search and User Administration permissions can assign and reassign users to an Evidence Group. This can be done from the User Details Page, User Search Page, the Add User Page, or Import User Page.

To assign a user to an Evidence Group on the User Details Page, select the appropriate group in the user's Account Details section.

SHOE, DAVE (98146)

This user account is currently unlocked.

UNLOCK ACCOUNT

Reset this user's Password and Security Questions. The user will be emailed a temporary password. Once they sign in, they will be forced to set up their new password and security questions.

RESET CREDENTIALS

Deactivate this user's account, with the option to reassign evidence and devices to another user. Account may be reactivated at a later time.

DEACTIVATE USER

ACCOUNT DETAILS

USERNAME	dshoe
FIRST NAME	Dave
LAST NAME	Shoe
BADGE ID	98146
EVIDENCE GROUP	12th Precinct - Detectives
EMAIL ADDRESS	daveshoe@gmail.com
EXTERNAL ID	DS999
USER ROLE	User (Basic) ▼

SAVE

To set the Evidence Group for one or more users from the User Search Page, find and select the appropriate users in the user list, click **Update Evidence Group**, and then select the appropriate Evidence Group.

The screenshot displays the 'ADMIN' section of the Axon Evidence interface. Under the 'ALL USERS' tab, there are search filters for LAST NAME, FIRST NAME, EMAIL, GROUP, EVIDENCE GROUP, RANK, ROLE, STATUS, BADGE ID, DATE, FROM, and TO. A blue 'SEARCH' button is present. Below the search filters, a row of action buttons is shown: UPDATE ROLE, UPDATE EVIDENCE GROUP (highlighted with a red box), REINVITE USERS, DEACTIVATE USERS, REACTIVATE USERS, RESET PASSWORD, and EXPORT. Below these buttons, it indicates '6245 Records Found | 3 records selected'. At the bottom, a table header is visible with columns: NAME, BADGE ID, ROLE, TIER, LAST ACTIVE, INVITED DATE, DEACTIVATED DATE, and STATUS.

To assign a new user to an Evidence Group when they are added to the system, select the appropriate group on the Add User page.

The screenshot shows the 'Add User' form in the 'ADMIN' section. The form includes fields for FIRST NAME, LAST NAME, BADGE ID, EVIDENCE GROUP (highlighted with a red box), USERNAME, EMAIL ADDRESS, USER ROLE, STATUS, and EXTERNAL ID. There are 'CANCEL' and 'ADD' buttons at the bottom. A note at the top left of the form states '* Indicates required field'.

To assign new users to an Evidence Group when importing them from a text or CSV file, enter the appropriate Evidence Group ID in the Evidence Group column. The group ID is the External ID shown on the group page.

	A	B	C	D	E	F	G	H
1	FIRST NAME	LAST NAME	EMAIL	BADGE ID	USERNAME	STATUS	EXTERNAL ID	EVIDENCE GROUP
2	John	Doe	johnd@taser.com	123456	johnd@taser.com	Active		
3	Jane	Doe	janed@taser.com	789012	janed@taser.com	Active		GroupId
4								

Manually Assigning Evidence to an Evidence Group

All evidence recorded by users that are assigned to an Evidence Group is automatically assigned to the recording user's evidence group.

The Evidence Group information for a piece of evidence is included in the Evidence Created, Evidence Deleted, and Uncategorized Evidence reports. These reports can be filtered to only show evidence from a selected Evidence Group.

Users assigned to Roles with the Evidence Search and Edit Evidence Group permissions can manually assign or reassign evidence to an Evidence Group from the associated Evidence Detail Page or the Evidence Search Page.

To manually assign or reassign evidence to an Evidence Group from the Evidence Detail Page, go to the page and select the appropriate Evidence Group.

The screenshot displays the Axon Evidence web application interface. The top navigation bar includes tabs for EVIDENCE, CASES, INVENTORY, REPORTS, ADMIN, and HELP. Below this, a secondary navigation bar shows options like ALL EVIDENCE, MY EVIDENCE, SHARED EVIDENCE, EVIDENCE MAP, IMPORT EVIDENCE, and CITIZEN EVIDENCE. The main content area features a video player showing a cityscape. To the right of the video player, there is a 'MANAGE EVIDENCE ACCESS' section with 'INSIDE MY AGENCY' and 'OUTSIDE MY AGENCY' tabs. Below this is a 'METADATA' section with fields for 'Assigned To', 'Recorded On', 'Uploaded On', 'Deletion Scheduled For', and 'File Size'. At the bottom right, there is a red-bordered box containing the 'Evidence Group' field, which is currently empty.

To manually assign or reassign evidence to an Evidence Group from the Evidence Search page, find and select the appropriate evidence in the search results, click **Update Evidence Group**, and then select the appropriate Evidence Group.

The screenshot shows the Axon Evidence Search interface. At the top, there's a navigation bar with tabs: EVIDENCE, CASES, INVENTORY, REPORTS, ADMIN, and HELP. Below this, there's a sub-navigation bar with options: ALL EVIDENCE, MY EVIDENCE, SHARED EVIDENCE, EVIDENCE MAP, IMPORT EVIDENCE, and CITIZEN EVIDENCE. The main search area includes fields for ID, TITLE, USER OR GROUP, DATE (with Start and End date pickers), CATEGORY (a dropdown), and TAG (a dropdown). There are buttons for 'RESET FILTERS' and 'SEARCH'. Below the search filters, there's a 'SHOW ADVANCED SEARCH' link. A row of action buttons is displayed: UPDATE ID, ADD CATEGORY, REASSIGN, REDACT, DOWNLOAD, MANAGE ACCESS, DELETE, RESTORE, and EXPORT. The 'UPDATE EVIDENCE GROUP' button is highlighted with a red box. Below the action buttons, it shows '32,319 ITEMS FOUND'. At the bottom, there's a 'VIEW TYPE' section with 'GALLERY' and 'TABLE' options, and a 'SORT BY' section with 'Recorded On' and 'SORT ORDER' options.

Command Hierarchy

The Command Hierarchy feature enables agency administrators to model their agency's command structure and use it as a single source-of-truth across all Axon products. Command Hierarchy provides Axon products, like Axon Evidence and Axon Performance, with the hierarchy context to drive permissions, workflows, reports and team configurations. Previously agencies were unable to properly express their command structure and had to construct it multiple times across each Axon product they use. This resulted in higher onboarding and administrative costs for the agencies.

The Command Hierarchy reflects the command structure of the agency, with a hierarchical tree of command levels, starting with the agency group at the top. Agency administrators can add groups to the Command Hierarchy for each command level in the organization to form a hierarchical tree that represents their organization structure. Users and Monitors are then added to these Groups to reflect their respective place in the command structure.

Command Hierarchy Permissions

The Command Hierarchy feature adds three new Role Permissions in Axon Evidence.

Command Hierarchy Management Permission

The **Manage Command Hierarchy** permission allows a user to add, edit, or remove groups from the Command Hierarchy. This includes importing groups using a CSV file.

The Manage Command Hierarchy permission requires that the role has the Create/Edit Groups permission set to Allowed.

▶ Command Hierarchy	
Manage Command Hierarchy	<input checked="" type="radio"/> Allowed <input type="radio"/> Prohibited

Command Hierarchy Evidence Management Permissions

There are two Command Hierarchy permissions associated with Evidence Management.

The **Access evidence in their Command** permission allows a user to perform an action (view, edit, etc.) on evidence where the Evidence Group is set to their Command Hierarchy Group or a subordinate (child) group.

The **Access evidence uploaded by users in their Command** permission allows a user to perform an action (view, edit, etc.) on evidence that was uploaded by users in their Command Hierarchy Group and subordinate (child) groups.

Both permissions require that the role has the appropriate Evidence Management permissions (View Unrestricted Evidence, View Restricted Evidence, View Confidential Evidence, Apply and Remove Access Class, Edit and Edit Evidence Group) set to Their group and their own.

Access evidence in their Command	<input checked="" type="radio"/> Allowed <input type="radio"/> Prohibited
Access evidence uploaded by Users in their Command	<input checked="" type="radio"/> Allowed <input type="radio"/> Prohibited

Creating a Command Hierarchy

Command Hierarchy can be created in Axon Evidence manually or by a CSV import. Command Hierarchy can also be created by using the Axon Evidence Partner API. See the Axon Evidence Partner API Guide for information on using the API with Command Hierarchy.

Command Hierarchy uses Groups to create the agency hierarchy by adding a top-level group, then adding child (subordinate) groups below the top-level group. Additional groups are then added below the initial groups. groups can be moved and edited as needed to reflect your agency's command structure.

Manually Creating a Command Hierarchy

1. On the menu bar click **Admin** and then, under Users, click **Command Hierarchy**.
2. Click Build Command Hierarchy.

3. Type the name of first group you want to add.

If your agency already has existing groups, when you begin typing the group name a list of existing groups is shown. Select a group name to add that group.

4. After adding the first group, click a **+** icon at the appropriate level to add a new child group.

Type the group name. If your agency already has existing groups, when you begin typing the group name a list of existing groups is shown. Select a group name to add that group.

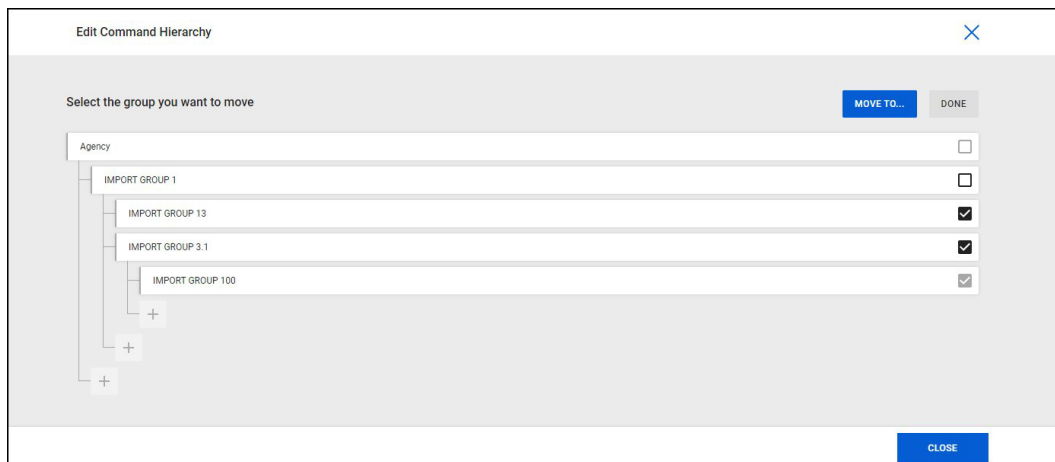
Alternately, you can use the ... (More Actions) menu on the right side of a group line to add a new child group. The More Actions menu also allows you to edit the name of a

group or remove a child group from the hierarchy. At the top level group the menu allows you to add a new top-level group.



You can also use the Move Groups option to move groups after adding them. Click **Move Groups**, select the groups you want to move, and then click **Move To**.

Note that child groups are automatically selected when their parent group is selected.



In the Move groups section on the right side of the page, choose the parent group for the selected groups and click **Move Here**.

5. When you have completed adding your groups, click **Close**.

Importing a Command Hierarchy

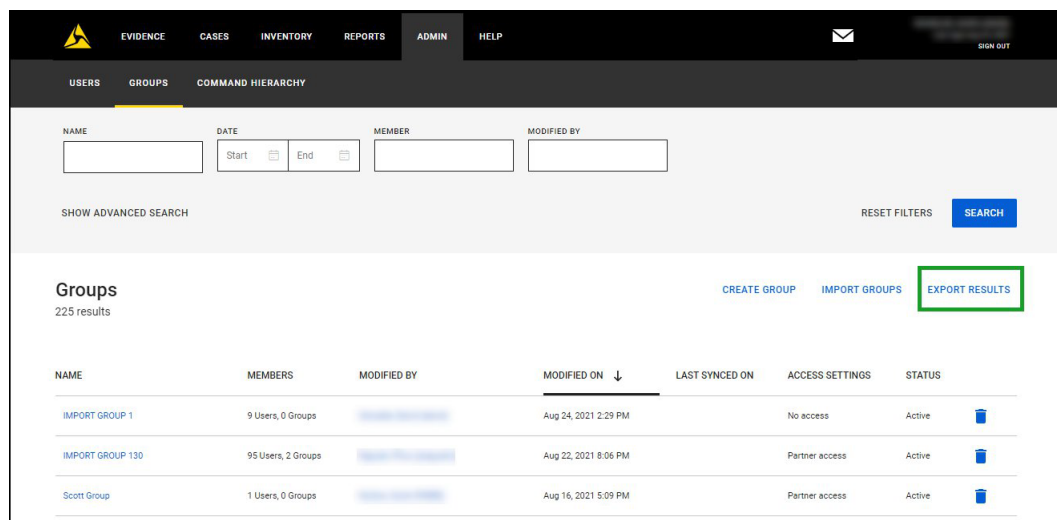
You can create your command hierarchy in Axon Evidence by using a CSV file to import group information.

If your Axon Evidence Account already has exiting Groups, you can export the group information as a CSV file and edit the file to build your hierarchy. If you do not have groups set up, you can use the import groups functionality to add groups and build your hierarchy at the same time.

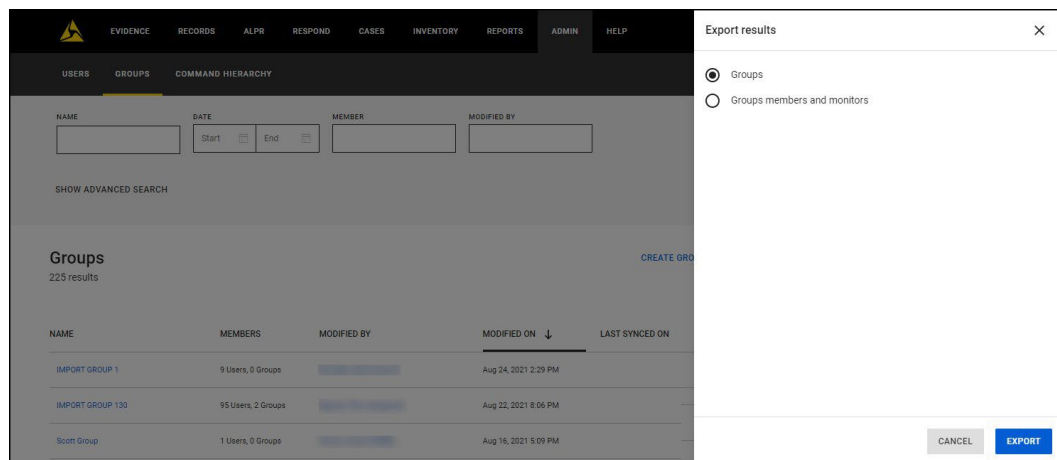
Exporting and Editing a CSV file

Use this process if you already have groups in Axon Evidence.

1. On the menu bar click **Admin** and then, under Users, click **Groups**.
2. On the groups page, click **Export Results**.



3. On the right side of the page, select **Groups** and click **Export**. A CSV file with all the groups in your agency is downloaded.



4. Open the exported CSV file.

5. Add the hierarchy information in the PARENT_EXTERNAL_ID column.
 - For the top-level group, enter **head** in the PARENT_EXTERNAL_ID column.
 - for child (subordinate) groups, enter the EXTERNAL_ID value for the parent group in the PARENT_EXTERNAL_ID column.

	A	B	C	D	E
1	EXTERNAL_ID	NAME	SHARE_ACCESS	PARENT_EXTERNAL_ID	STATUS
2	13	Agency	FORBIDDEN	head	Active
3	13-D1	District 1	FORBIDDEN	13	Active
4	13-D2	District 2	FORBIDDEN	13	Active
5	13-D1-G	District 1 Groups	INTERNAL	13-D1	Active
6	13-D1-G-A	Group Able	INTERNAL	13-D1-G	Active
7	13-D1-G-B	Group Bravo	INTERNAL	13-D1-G	Active
8	13-D1-G-C	Group Charlie	INTERNAL	13-D1-G	Active
9					

Example: In the example CSV file above: Agency is the top-level group and has **head** in the PARENT_EXTERNAL_ID column, District 1 is subordinate to Agency and has **13** (the EXTERNAL_ID for Agency) in the PARENT_EXTERNAL_ID column, and Group Able is subordinate to District 1 Groups and has **13-D1-G** (the EXTERNAL_ID for District 1 Groups) in the PARENT_EXTERNAL_ID column.

6. Save the CSV file. Go to the Importing a CSV file process.

Creating a CSV file

Use this process if you do not have existing groups in Axon Evidence.

1. On the menu bar, click **Admin** and then, under Users, click **All Groups**. On the Groups page click **Import Groups**.
2. With the Import Option set to Create groups or Synchronize groups, click **Download Example File** to save the example csv file to your computer.
3. Make a copy of the ImportGroups.csv file and assign it a meaningful file name.

This new file is your groups CSV file.

4. Open the CSV file.
5. Delete the second, third, and fourth rows. Do not delete the first row. Evidence.com expects the first row to contain the column names.
6. For every group that you want to add, include a row in the file that specifies values for the group, as described in the following table. Ensure that each value is in the cell beneath the applicable header.

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:

Column	Header Value	Value
A	EXTERNAL_ID	<p>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.</p> <p>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.</p> <p>To find the external group ID for an existing group, view the Group Profile page for the group.</p> <p>You can also simply assign a descriptive name.</p> <p>Valid external group IDs can be up to 255 characters.</p>
B	NAME	<p>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.</p> <p>Valid group titles can be up to 128 characters.</p>
C	SHARE_ACCESS	<p>Sets the access levels for the group and corresponds to the Manage Access Settings. Valid values are the following three words:</p> <ul style="list-style-type: none"> • 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.
D	PARENT_EXTERNAL_ID	<p>The EXTERNAL_ID value for this group's parent group. If this is the top-level group, the value should be head.</p>

7. Save the CSV file. Go to the Importing a CSV file process.

Importing a CSV File

1. On the menu bar click **Admin** and then, under Users, click **All Groups**.
2. On the groups page, click Import Groups.
3. On the Import Groups page select Synchronize groups.

Import groups

IMPORT OPTION
Synchronize groups

This option will replace all of your groups in the system with exactly what is in the CSV file. Any group that is not referenced will be deleted and cannot be reverted.

[DOWNLOAD EXAMPLE FILE](#)

Upload file
Accepted file type is comma separated value (.csv).

[SELECT FILE](#)

[UPLOAD](#)

4. Click **Select File** and select the CSV file with your group and hierarchy information.
5. Click **Upload**.
6. When the upload is complete, Click **Command Hierarchy** and confirm the hierarchy has been updated.

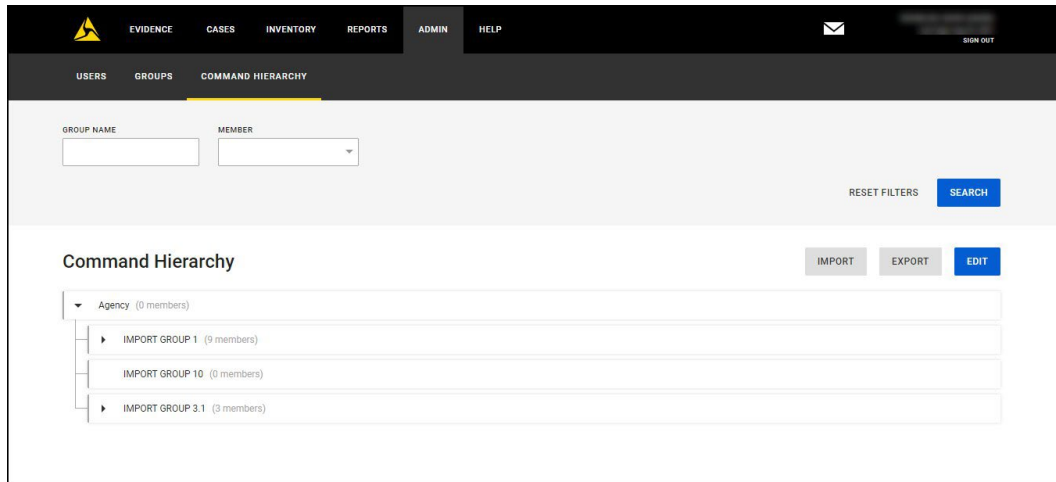
Editing a Command Hierarchy

Command Hierarchy can be edited in Axon Evidence manually or by importing changes in a CSV file. Command Hierarchy can also be edited by using the Axon Evidence Partner API. See the Axon Evidence Partner API Guide for information on using the API to work with Command Hierarchy.

Manually Editing a Command Hierarchy

1. On the menu bar click **Admin** and then, under Users, click **Command Hierarchy**.

2. Click **Edit**.



3. Click a **+** icon at the appropriate level to add a new child group.

Type the group name. If your agency already has existing groups, when you begin typing the group name a list of existing groups is shown. Select a group name to add that group.

Alternately, you can use the ... (More Actions) menu on the right side of a group line to add a new child group. The More Actions menu also allows you to edit the name of a group or remove a child group from the hierarchy. At the top level group the menu allows you to add a new top-level group.



You can also use the Move Groups option to move groups after adding them. Click **Move Groups**, select the groups you want to move, and then click **Move To**.

Note that child groups are automatically selected when their parent group is selected.

Dialog box titled "Edit Command Hierarchy". It contains a section "Select the group you want to move" with a "MOVE TO..." button and a "DONE" button. Below this is a tree structure of groups. The "Agency" group is selected, and its child groups, "IMPORT GROUP 1", "IMPORT GROUP 13", "IMPORT GROUP 3.1", and "IMPORT GROUP 100", are also selected. The "MOVE TO..." button is highlighted.

In the Move groups section on the right side of the page, choose the parent group for the selected groups and click **Move Here**.

4. when you have completed adding your groups, click **Close**.

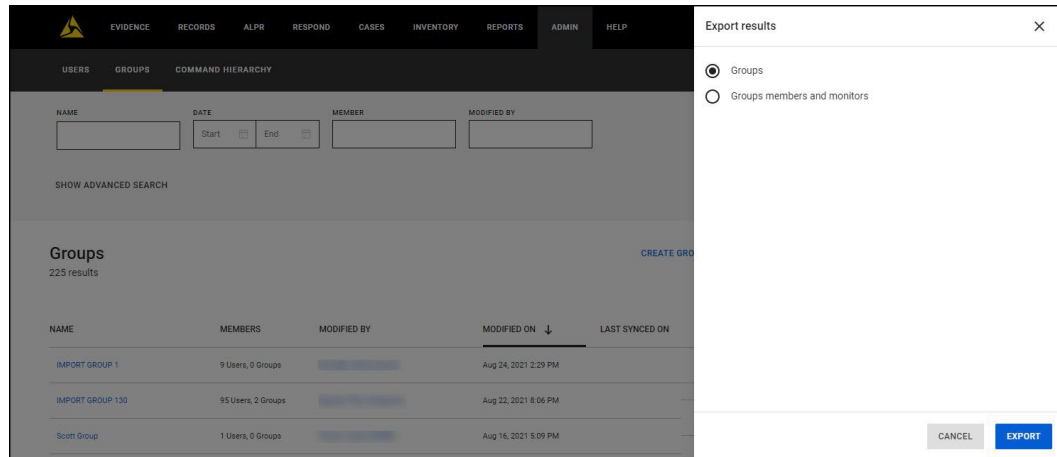
Importing Updates for a Command Hierarchy

1. On the menu bar click **Admin** and then, under Users, click **Groups**.
2. On the groups page, click **Export Results**.

Groups page screenshot. The "EXPORT RESULTS" button is highlighted with a green box. The page shows a table of groups with columns for Name, Members, Modified By, Modified On, Last Synced On, Access Settings, and Status.

NAME	MEMBERS	MODIFIED BY	MODIFIED ON	LAST SYNCED ON	ACCESS SETTINGS	STATUS
IMPORT GROUP 1	9 Users, 0 Groups	[User Name]	Aug 24, 2021 2:29 PM		No access	Active
IMPORT GROUP 130	95 Users, 2 Groups	[User Name]	Aug 22, 2021 8:06 PM		Partner access	Active
Scott Group	1 Users, 0 Groups	[User Name]	Aug 16, 2021 5:09 PM		Partner access	Active

- On the right side of the page, select **Groups** and click **Export**. A CSV file with all the groups in your agency is downloaded.

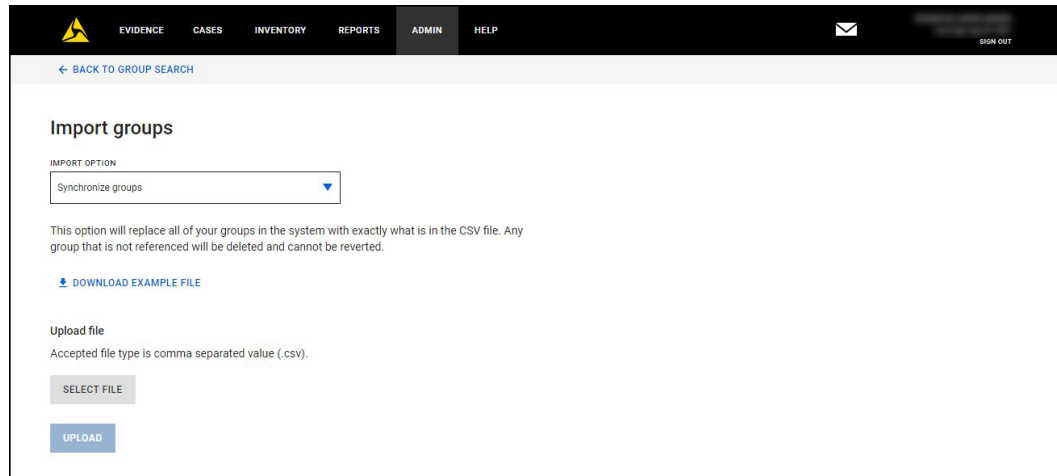


- Open the exported CSV file.
- Add the hierarchy information in the PARENT_EXTERNAL_ID column.
 - For the top-level group, enter head in the PARENT_EXTERNAL_ID column.
 - for child (subordinate) groups, enter the EXTERNAL_ID value for the parent group in the PARENT_EXTERNAL_ID column.

	A	B	C	D	E	
1	EXTERNAL_ID	NAME	SHARE_ACCESS	PARENT_EXTERNAL_ID	STATUS	
2	f4fe840a-5408-46b6-b5aa-9608c2776c69	Agency	FORBIDDEN	head	Active	
3	c32411ab-d43b-49cf-8fd7-f7ea75108078	Central	FORBIDDEN		Active	
4	fa516031-6c0f-4830-8a90-3aa74c04155a	Financial Investigations	FORBIDDEN		Active	
5	2eb75ad7-7f8c-4f54-9e64-8101fdad855f	Narcotics	FORBIDDEN		Active	
6	edad30e5-7e2a-470d-9166-0d1b38c75e7f	North Central	FORBIDDEN		Active	
7	e32f2779-199c-4d2d-aa0f-3f8950b3b0e3	Northeast	FORBIDDEN		Active	
8	ca5423fa-1149-4f1d-bbdf-a7a7323c05ad	Northwest	FORBIDDEN		Active	
9	25ad8203-a0d7-49a7-9ec4-33e8524459ac	Patrol Division	FORBIDDEN		Active	
10	f2d9e313-3a5c-4795-a3ca-5def5f64f608	test	FORBIDDEN		Active	
11	b3fa1a84-ee93-483b-9b5b-e84a207d46cb	testtest	ANY		Active	
12	05b1cfff-c484-44da-a63b-4244baa8bb14	Zone 1A	FORBIDDEN		Active	
13	711ae7aa-90e2-44a4-9a6d-3fcfc55d9cad	Zone 2B	FORBIDDEN		Active	
14	54afd3a0-af63-40fb-9f1a-9ca5bc08c2b0	Zone 3C	FORBIDDEN		Active	
15						

- Save the CSV file.
- On the menu bar click **Admin** and then, under Users, click **All Groups**.
- On the groups page, click **Import Groups**.

9. On the Import Groups page select **Synchronize groups**.



10. Click **Select File** and select the CSV file with your group and hierarchy information.
11. Click **Upload**.
12. When the upload is complete, Click **Command Hierarchy** and confirm the hierarchy has been updated.

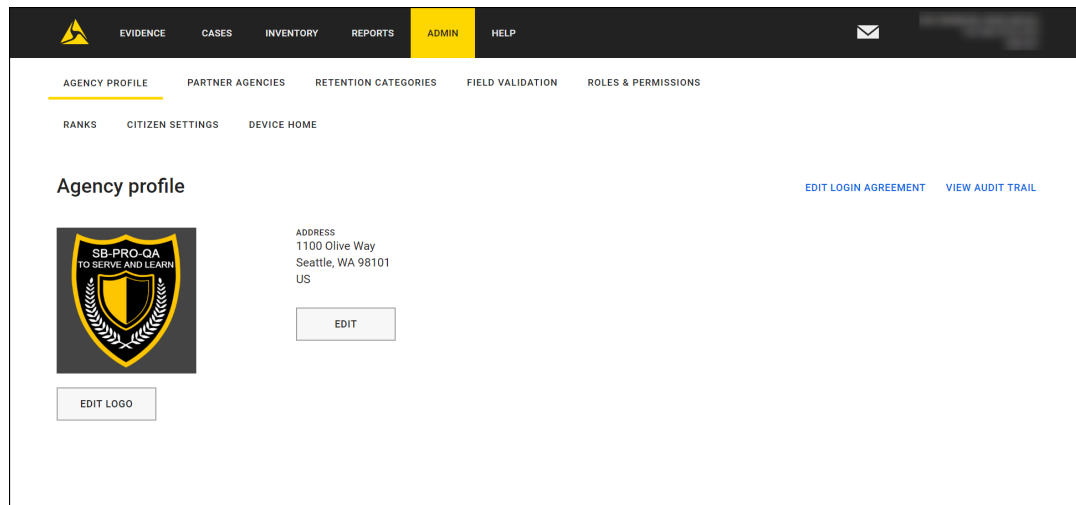
Agency Profile

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 Address

1. On the menu bar, click **Admin** and then under Agency Settings, click **Agency Profile**.

The Agency Profile page appears.



2. Under Address, click **Edit**.
3. In the boxes and lists provided, specify the agency street address.
4. When you have finished editing the address, click **Save**.

On the notification message box, click **Close**.

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, 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 **Edit Logo**.
3. If you want to specify a new logo, click **Upload**, select the logo file, and click **Open**.

The file uploads to Evidence.com.

4. If you want to remove the logo, click **Remove**. The system asks you to confirm that you want to remove the logo.
5. After you have completed your changes, click **Save**.
6. On the notification message box, click **Close**.

The Agency Profile page shows the logo that you uploaded or, if you deleted the logo, shows a placeholder Evidence.com logo.

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
- Devices and Applications 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 opens that provides options for viewing the entire audit trail or a portion of the audit trail.

3. Select the date range that you want to view. If you select Custom Date Range, you can specify a start and end date. Click **Download**.

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.

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

Partner Agency Administration

Axon Evidence makes it easy for your users to share evidence and cases with other Axon Evidence 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 Axon Evidence agency, the Partner Agencies page has two lists that administrators can use to control how your agency collaborates with its partner agencies.

- **Can Share to My Agency** — The list of agencies that can share evidence and cases with your users and groups. These agencies have accepted your invitation and your agency appears on their My Agency Can Share To list.

When a user in one of these agencies wants to share cases and evidence with your agency, your agency's users and groups are available and can be found when the user in the other agency searches for people and groups to share with.

Partner agencies




[Learn More](#)

Can Share to My Agency

My Agency Can Share To

35 results

ADD AGENCY

Agency Name	City	State	Status ↑	Action
Regional Support Management	Scottsdale	AZ	Accepted	
Axon - walkthrough	Scottsdale	AZ	Accepted	
Axon - Enterprise	Scottsdale	AZ	Accepted	

- **My Agency Can Share To** — The list of agencies whose users and groups are available for your agency to share with. They have accepted your invitation and your agency appears on their Can Share to My Agency 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.




Partner agencies

[Learn More](#)

Can Share to My Agency

My Agency Can Share To

31 results

Agency Name	City	State	Status ↑	Action
TASER Axon	Scottsdale	AZ	Accepted	
Axon Interview Room (AIR) Demo	Scottsdale	AZ	Accepted	
Axon Prosecutor Demo Account	Scottsdale	AZ	Accepted	

Sharing with Partner Agencies

Users who are allowed the Share with Partner Agencies permission can share cases with agencies on your My Agency Can Share To list. Users who are allowed the Share Externally to Authenticated Users permission can share evidence with agencies on your My Agency Can Share To 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.

Note: Administrators of agencies that you add to the Can Share to My Agency list receive a notification email. Before users in your agency can share a case with the partner agency, an administrator from the partner agency must accept the invitation.

1. On the menu bar, click **Admin** and then under Agency Settings, click **Partner Agencies**.

The Partner Agencies page is shown.

2. Under **Can Share to My Agency**, click **Add Agency**.

The Add Agencies-panel opens on the right-side of the page.

The screenshot shows the 'Add Agencies' panel. It contains input fields for Agency Name, City, State (dropdown), and ZIP. There is also a Country dropdown menu. Below these fields are 'RESET FILTERS' and 'SEARCH' buttons. A table titled 'Agencies' is shown with columns for Agency Name, City, State, and Status. The table is currently empty, and a message prompts the user to search for an agency using the filters above. A 'DONE' button is located at the bottom right of the panel.

3. Use the filters at the top of the panel to search for the agency you want to share information with.
4. In the search results, on the same line as the agency name click **Add**.
5. The system asks you to confirm that you want to send the partner agency request.
Click **Send Invitation** to send the invitation and continue.
6. The system sends the invitation and returns to the Add Agencies-panel.

You can repeat steps 3 – 5 to send additional partner requests or click **Done** to return to the Partner Agencies page.

Accepting or Rejecting an Invitation to Collaborate with an Agency

When another agency invites you to share evidence and cases, Axon Evidence 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 is shown.

2. In the **My Agency Can Share To** 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**. The system asks you to confirm that you want to accept the request.

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**. The system asks you to confirm that you want to reject the request.


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.

Removing an Agency from your Can Share to My Agency List

1. On the menu bar, click **Admin** and then under Agency Settings, click **Partner Agencies**.

The Partner Agencies page is shown.

2. In the Can Share to My Agency list, find the agency you want to remove and click the  (delete) icon on the same line.


3. The system asks you to confirm the removal of the agency from the list.

Your agency can no longer receive shared cases and evidence from the other agency.

Removing an Agency from your My Agency Can Share To List

1. On the menu bar, click **Admin** and then under Agency Settings, click **Partner Agencies**.

The Partner Agencies page is shown.

2. Click the My Agency Can Share To list, find the agency you want to remove and click the  (delete) icon on the same line.
3. The system asks you to confirm the removal of the agency from the list.

Your agency can no longer send shared cases and evidence to the other agency.

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 and Confidential Categories

The Categories feature provides the ability to apply the Restricted or Confidential access class to evidence that is especially sensitive. In order to view evidence assigned to a Restricted or Confidential access class, users must be on the evidence access list or assigned a role that has the appropriate permission.

Note: If a user does not have permission to apply the Restricted or Confidential access class, then the user will not be able to assign evidence to a category that applies the access class change in Axon Evidence. Users applying categories using Axon mobile or desktop apps are not restricted from assigning categories.

By default, all new and pre-configured categories are not restricted or confidential categories.

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

Set the length of time that evidence with this category is retained before being placed in the deletion queue.

Evidence with multiple categories uses the longest retention time. Uncategorized evidences uses the Uncategorized category settings.

Evidence included in a Case is not placed in the deletion queue.

0	Until Manually Deleted ▼
	Until Manually Deleted
	Days
	Weeks
	Years

- If you do not want Evidence.com to initiate the deletion of evidence in this category, leave **Until Manually Deleted** as the selection.
5. Select if the new category should **Include Access Restriction**. Enabling this option automatically applies the selected access class to the evidence and limits user access to those users on the access list or with the appropriate Restricted or Confidential access class permission.

After enabling the option, select the access class, **Restricted** or **Confidential**, that is applied to the evidence.

Note: If a user does not have permission to apply the Restricted or Confidential access class, then the user will not be able to assign evidence to a category that applies the access class change in Axon Evidence. Users applying categories using Axon mobile or desktop apps are not restricted from assigning categories.

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.

Task	Steps
Change the category name	Under Name , type the new name.
Set a retention period for evidence assigned to this category	<ol style="list-style-type: none"> 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 .

Task	Steps
Enable Include Access Restriction setting for evidence assigned to the category	Enable Include Access Restricted and select the access class, Restricted or Confidential , that is applied to the evidence.
Change Include Access Restriction setting for evidence assigned to the category	<p>Select the access class, Restricted or Confidential, that is applied to the evidence.</p> <p>Note: If a user does not have permission to apply the Restricted or Confidential access class, then the user will not be able to assign evidence to a category that applies the access class change in Axon Evidence. Users applying categories using Axon mobile or desktop apps are not restricted from assigning categories.</p>
Remove Access Restriction from the category	Disable the Include Access Restricted option.

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.

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.

When Evidence ID field validation is enabled, it is also enforced when entering Evidence ID information in Axon View and Axon Capture with some limitations.

- Axon View – The body worn camera that is paired with the application must have connected to Evidence.com (through an Axon Dock or Evidence Sync) after the last Evidence ID field validation change was made.
- Axon Capture – The application must connect to Evidence.com and receive updates after the last Evidence ID field validation change was made.

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.

Field Validation

The field validation feature is used to ensure that Evidence.com users enter field information correctly. The feature uses a regular expression (regex) to set the expected format for the field and descriptor text to provide format information to users. When field validation is enabled for a field, the descriptor text appears as hint text in the appropriate Evidence.com field and as part of the error message.

For help creating a regular expression, please see the [Axon Help Center](#).

Badge ID

☐ Disabled

REGEX
/^ S/

DESCRIPTOR ?

CANCEL SAVE

Evidence ID

☐ Disabled

REGEX
/^ S/

DESCRIPTOR ?

CANCEL SAVE

Case ID

☐ Disabled

REGEX
/^ S/

DESCRIPTOR ?

CANCEL SAVE

2. Select the **Badge ID**, **Evidence ID**, and/or **Case 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**, **Evidence ID**, and/or **Case 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:

- Regular Expressions User Guide — <http://www.zytrax.com/tech/web/regex.htm>
- Debuggex, a regular expression debugger site — <https://www.debuggex.com/>

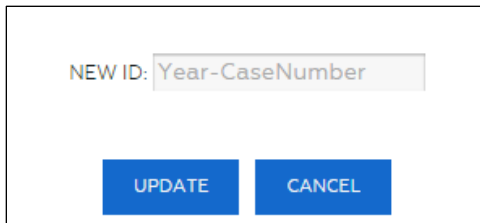
Example Regular Expressions

The following table provides a few examples of ID formats and regular expressions that match only IDs that comply with the ID format.

ID Format Example & Description	Matching Regular Expressions and Comments
YYYYMMDDnnnnnn Four-digit year, two-digit month, two-digit day, and 6-digit number.	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. / [^] 20\d\d(0[1-9] 1[012]) (0[1-9] [12] [0-9] 3[01]) [0-9]{6}\$/
YYYY-nnnnnn or YY-nnnnnn Four-digit year or two-digit year, a dash, and then a 6-digit number.	The following regular expression allows any year between 2000 and 2099, with or without 20 at the start of the ID. / [^] (20)?(\d\d)-[0-9]{6}\$/ 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. / [^] (20)?(15)-[0-9]{6}\$/
XX-XXXX Two characters, a dash, and then four characters.	The following regular expression allows any two alphanumeric characters, a dash, and then any four alphanumeric characters. / [^] [\w]{2}-[\w]{4}\$/

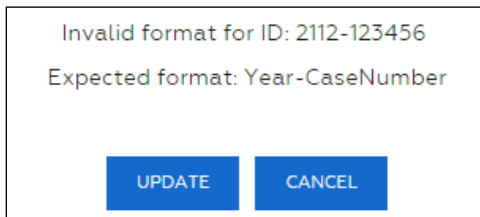
User Experience

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:



A dialog box with a light gray border. At the top, it says "NEW ID:" followed by a text input field containing "Year-CaseNumber". Below the input field are two blue buttons: "UPDATE" and "CANCEL".

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.



An error dialog box with a light gray border. It contains the text "Invalid format for ID: 2112-123456" in red. Below this, it says "Expected format: Year-CaseNumber" in gray. At the bottom are two blue buttons: "UPDATE" and "CANCEL".

Evidence Playback Settings

The Evidence Playback Settings page is used to set which Metadata Overlay information is shown by default and to set the position of the Viewed By watermark shown during video playback.

1. On the menu bar, click **Admin** and then click **Evidence Playback Settings**.

The Evidence Playback page is shown with the Overlay tab selected.

Evidence Playback Settings

Overlay | Watermark

Agency Info

Overlay	Display format	Display overlay by default
Agency Name	SB-PRO-QA	<input checked="" type="checkbox"/> Enabled

Evidence Metadata

Overlay	Display format	Display overlay by default
ID	Evidence ID Field	<input checked="" type="checkbox"/> Enabled
Recorded On	Time Zone	<input type="checkbox"/> Disabled
Activation Reason	Activation: Reason	<input type="checkbox"/> Disabled
Officer	Badge ID	<input checked="" type="checkbox"/> Enabled

Vehicle

Overlay	Display format	Display overlay by default
Speed		<input checked="" type="checkbox"/> Enabled

SAVE SETTINGS

- The Overlay tab is used to set the information that is shown by default during video playback. Use the toggle switch on the same line as the data to enable the information to be displayed by default.

The Display Format column shows the information that is displayed on the metadata overlay.

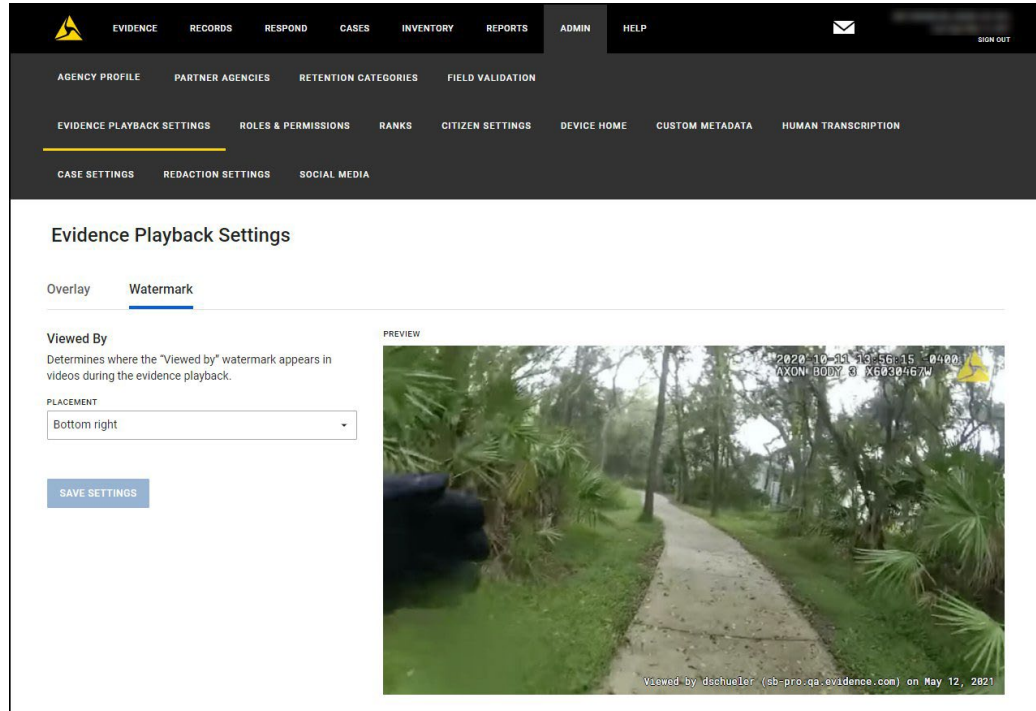
The Officer information format has three different options that can be shown.

Note: The information available in the Vehicle section depends on which version of Axon Fleet is used by your agency. Axon Fleet 1 and 2 agencies can only enable the Speed overlay information. Axon Fleet 3 agencies can enable the Speed, Lightbar, Brakes, and Siren overlay information. The Lightbar, Brakes, and Siren overlays show the associated letter (L, B, or S) on the overlay when that item is activated.

- After making any changes on the Overlay page, click **Save Settings** to save the changes.

- The Watermark tab set the position of the Viewed By watermark that is shown during video playback. the options are bottom left (default), bottom right, or center.

Currently, the Viewed By watermark position setting is only supported for videos.



- After making any changes on the Watermark page, click **Save Settings** to save the changes.

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.

Pre-Configured Role	Locked or Configurable	Required License Tier
Admin	Locked	Pro

Pre-Configured Role	Locked or Configurable	Required License Tier
User	Configurable	Basic (Pro if a Pro license permission is allowed)
Investigator	Configurable	Pro
Armorer	Configurable	Basic (Pro if a Pro license permission is allowed)
Lite User	Locked	N/A
Lite Armorer	Locked	N/A

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  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.

Ranks

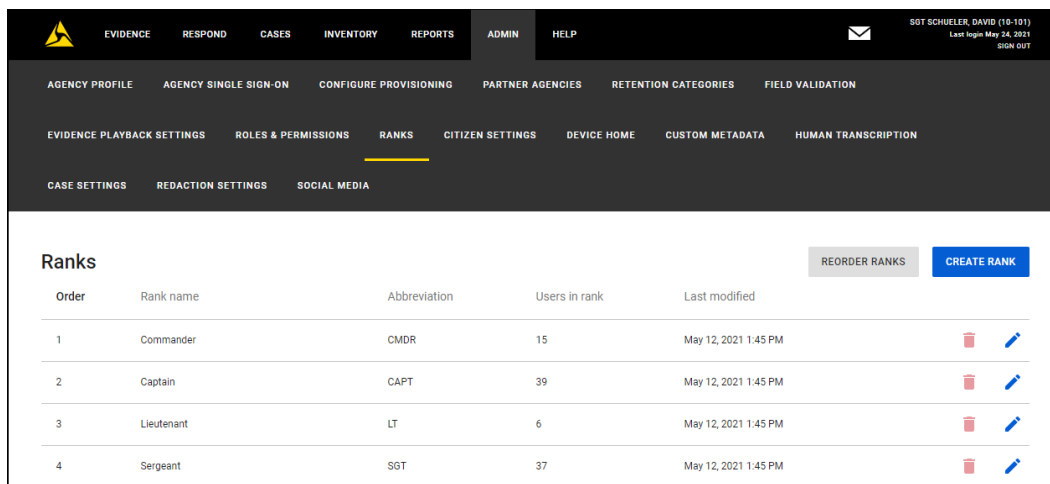
The Ranks section is used to create and manage agency ranks. The Rank attribute can be used as part of a user's profile, but Rank is not a required field for user management.

Rank can be added or changed in existing user profiles from the Manage User page. Ranks can also be added when the user is added or imported into Axon Evidence.com. See [User Administration](#) for more information on working with users.

Add a Rank

1. On the menu bar, click **Admin** and then, under Agency Settings, click **Ranks**.

The Ranks page is shown.



2. Click **Create Rank**. The Create Rank dialog box is shown.

Create Rank

NAME *

ABBREVIATION

CANCEL CREATE

3. Enter the **Name** for the new Rank. The name can be up to 256 characters in length.

Optionally, enter an **Abbreviation** for the new Rank. The abbreviation can be up to 256 characters in length.

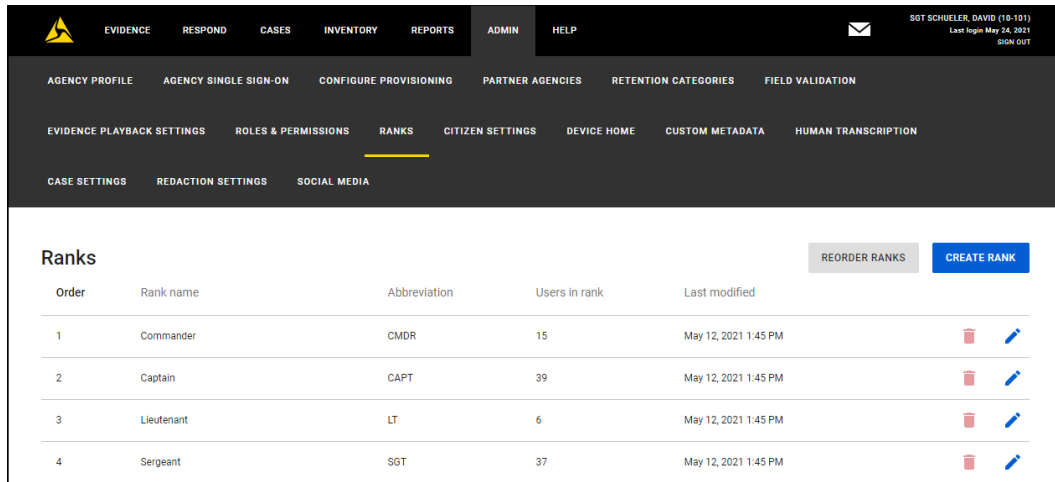
4. Click **Create**.

The system confirms the new Rank was created. Click **Close** to return to the Ranks page.

Edit a Rank

1. On the menu bar, click **Admin** and, then under Agency Settings, click **Ranks**.

The Ranks page is shown.



- Find the Rank you want to edit and click the edit icon (✎) on the same line. The Update Rank dialog box is shown.

Edit Rank

NAME *

Sergeant

ABBREVIATION

SGT

CANCEL UPDATE

- Update the Rank Name and Abbreviation information as needed.
- Click **Update**.

The system confirms the Rank was updated. Click **Close** to return to the Ranks page.

Delete a Rank

You cannot delete a Rank if users are still assigned to the Rank. Before deleting a Rank, ensure that no users are assigned to that rank. You can do check this by going to the All Users page, searching for users with the rank you want to delete, and editing the rank information for users as needed.

- On the menu bar, click **Admin** and then under **Agency Settings**, click **Ranks**.

The Ranks page is shown.

Order	Rank name	Abbreviation	Users in rank	Last modified
1	Commander	CMDR	15	May 12, 2021 1:45 PM
2	Captain	CAPT	39	May 12, 2021 1:45 PM
3	Lieutenant	LT	6	May 12, 2021 1:45 PM
4	Sergeant	SGT	37	May 12, 2021 1:45 PM

- Find the Rank you want to delete and click the delete icon () on the same line.
- The system asks you to confirm the deletion.

Note: You cannot delete a rank if any users are assigned to the rank.

Delete rank: aaa?

- Click **Delete**.

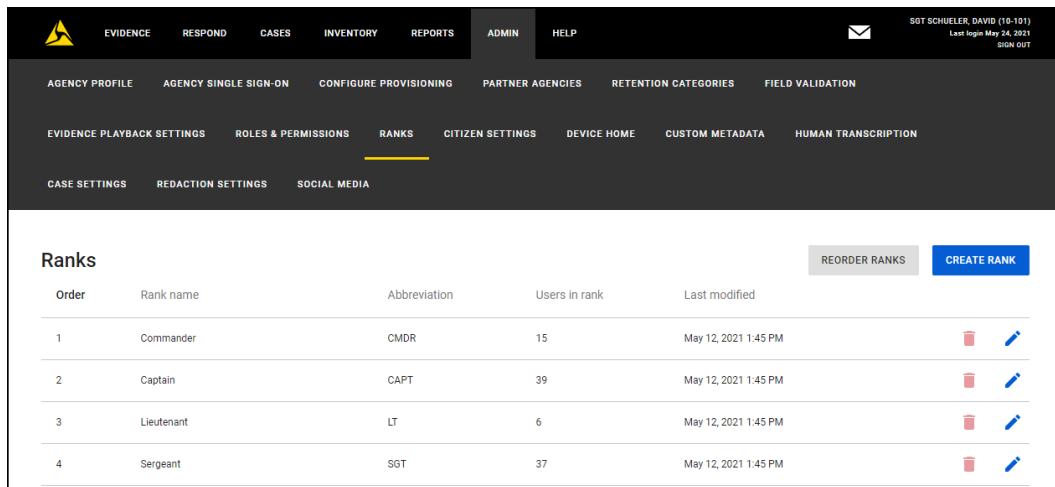
The system confirms the Rank was deleted. Click **Close** to return to the Ranks page.

Reorder Ranks

Note: Rank Order does not have any current use, but is part of the upcoming Command Hierarchy functionality.

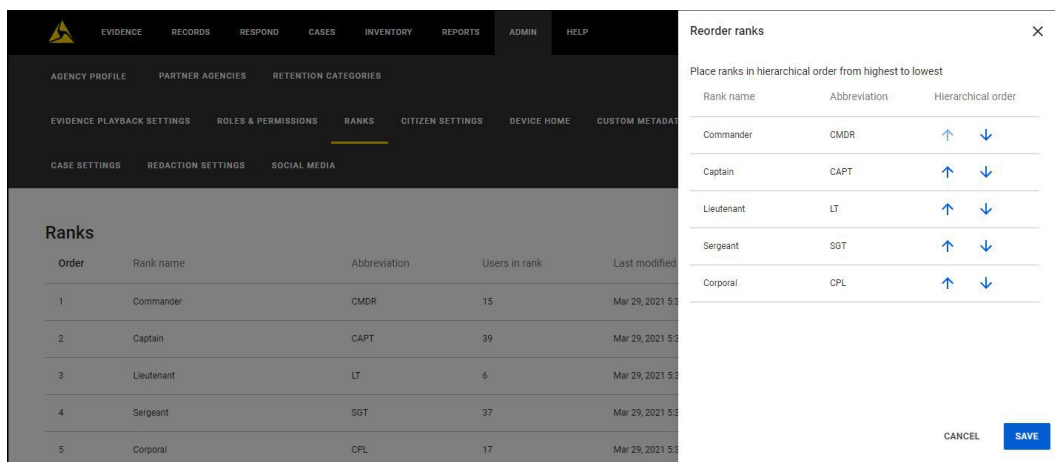
- On the menu bar, click **Admin** and then, under Agency Settings, click **Ranks**.

The Ranks page is shown.



Order	Rank name	Abbreviation	Users in rank	Last modified
1	Commander	CMDR	15	May 12, 2021 1:45 PM
2	Captain	CAPT	39	May 12, 2021 1:45 PM
3	Lieutenant	LT	6	May 12, 2021 1:45 PM
4	Sergeant	SGT	37	May 12, 2021 1:45 PM

- Click **Reorder Ranks**. The Reorder Ranks screen is shown on the right side of the page.



Rank name	Abbreviation	Hierarchical order
Commander	CMDR	↑ ↓
Captain	CAPT	↑ ↓
Lieutenant	LT	↑ ↓
Sergeant	SGT	↑ ↓
Corporal	CPL	↑ ↓

- Use the Hierarchical order arrows to move the ranks up or down. The highest rank should be at the top of the list and other ranks placed in descending order.
- Click **Save** to save the changes.

The system asks you to confirm the changes. Click **Close** to return to the Ranks page.

Citizen Settings

Agency Axon Evidence 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 then 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 Axon Evidence.

Configure Citizen Settings

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Citizen Settings**.

The Citizen Settings page is shown.

2. Set the **Help Contact Settings** options.

Help Contact Settings

Enter up to three contact methods for community members to use if they have questions about their evidence submission. The contact methods are shown at the bottom of all Axon Citizen web pages community members visit.

☒ Enable contact information

name@email.com	Email ▼
555-555-5555	Phone ▼
www.axonpd.com/contact	Website ▼

This setting allows you to show up to three ways community members can contact your agency in the footer of Axon Citizen evidence upload pages.

To enable the option, toggle **Enable contact information** to on. Then enter the contact method information (email address, phone number, or website URL) and select the contact method type (Email, Phone, or Website).

3. Set the **Retention Period for Declined Submission** options.

Retention Period for Declined Submissions

Evidence declined during triage uses the default category retention period unless a custom retention period is specified below.

☒ Use custom retention period

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. Select the **Retention Period** interval (Days, Weeks, Years) and enter the Retention Period length.

4. In the Individual Invite Settings section, select if the ID, Category, and Description fields are required, optional, or not shown to senders for individual invitations.

Individual Invite Settings

Incident Info

ID Field

☐ Do Not Show
 ☒ Not Required
 ☐ Required

Categories Field

☐ Do Not Show
 ☒ Not Required
 ☐ Required

Description Field

☐ Do Not Show
 ☒ Not Required
 ☐ Required

- 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.
5. In the Community Member Info section, select if your agency will **Require contact information to be stored in Axon Evidence** for individual invites.

Public Portal Settings

Community Member Info

☒ Require contact information be stored in Axon Evidence

First Name

☒ Not Required
 ☐ Required

Last Name

☒ Not Required
 ☐ Required

Date of Birth

☒ Do Not Show
 ☐ Not Required
 ☐ Required

Enabling 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 Axon Evidence.

- If required, select the information fields that are required whenever contact information is stored in Axon Evidence for individual invites.
6. Optionally, select to hide the Date of Birth field for individual invites by selecting **Do Not Show**.
 7. Select the **Auto-Accept Submissions** setting for individual invites (blue = on).

Auto-Accept Submissions

When Auto-Accept is on, submitted files are automatically accepted and placed in Active status.
When Auto-Accept is off, submitted files are placed in Pending Triage status and can be manually accepted or declined.

☒ Auto-Accept submissions from individual invites

When on, submissions from individual invites are automatically accepted and place in active status. Otherwise, users must manually accept or decline each evidence submission.

8. In the Public Portals Settings section, select if your agency will **Require contact information to be stored in Axon Evidence** for portals.

Public Portal Settings

Community Member Info

☒ Require contact information be stored in Axon Evidence

First Name

☒ Not Required
 ☐ Required

Last Name

☒ Not Required
 ☐ Required

Date of Birth

☒ Do Not Show
 ☐ Not Required
 ☐ Required

- If required, select the information fields that are required whenever contact information is stored in Axon Evidence.
9. Optionally, select to hide the Date of Birth field for Public Portals by selecting **Do Not Show**.
 10. Click **Save Settings**.

The Citizen Settings are saved.

Device Home

The Device Home attribute is designed to help improve agency device inventory management. This attribute can help with inventory management and track where the device belongs. The Device Home attribute can be added to devices and then used to find

devices on the Axon Evidence.com Inventory search page, and to further help an agency track where devices are kept when they are not deployed with users.

Note: The Device Home attribute is only shown on the Inventory search page or device detail pages if your agency has at least one Device Home.

Add a Device Home

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Device Home**.

The Device Home page is shown.

The screenshot shows the Axon Evidence web interface. The top navigation bar includes 'EVIDENCE', 'CASES', 'INVENTORY', 'REPORTS', 'ADMIN' (highlighted), and 'HELP'. A user profile 'SCHUER, DAVID (DS101)' is in the top right. Below the navigation bar is a sub-menu with 'AGENCY PROFILE', 'AGENCY SINGLE SIGN-ON', 'CONFIGURE PROVISIONING', 'PARTNER AGENCIES', 'RETENTION CATEGORIES', 'FIELD VALIDATION', 'ROLES & PERMISSIONS', 'RANKS', 'CITIZEN SETTINGS', 'DEVICE HOME' (highlighted), 'MANAGED METADATA', and 'TRANSCRIPTION SETTINGS'. The main content area is titled 'Device Home' and contains a description: 'Device Home is provided to help with device inventory management. When device homes are created they will be visible within device search and on individual device profiles.' Below this is a 'DEVICE HOME MANAGEMENT' section with a 'CREATE DEVICE HOMES' button and a 'NEW DEVICE HOME' button. Under 'NEW DEVICE HOME', there are two input fields: 'DEVICE HOME NAME' with the value '12th Precinct' and 'POINT OF CONTACT' with the value 'Shoe, Dave (98146)'. There are edit and delete icons to the right of the 'POINT OF CONTACT' field.

2. Click **New Device Home**. The Create Device Home dialog box is shown.

The screenshot shows a 'Create Device Home' dialog box. It has a title bar 'Create Device Home'. Below the title bar are two input fields. The first is labeled 'DEVICE HOME NAME' and has a question mark icon. The second is labeled 'POINT OF CONTACT' and has a question mark icon. Below the 'POINT OF CONTACT' field is a dropdown menu with the text 'Enter last name, first name or badge ID'. At the bottom of the dialog box are two buttons: 'CANCEL' and 'CREATE'.

3. Enter the name for the new Device Home. The name can be up to 64 characters in length.

Optionally, enter a Point of Contact for the new Device Home. The Point of Contact must be a user in your agency's account.

4. Click **Create**.

The system confirms the Device Home was created. Click **Close** to return to the Device Home page.

Edit a Device Home

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Device Home**.

The Device Home page is shown.

2. Find the Device Home you want to edit and click the edit icon (✎) on the same line. The Update Device Home dialog box is shown.

3. Update the Device Home Name and Point of Contact information as needed.

4. Click **Update**.

The system confirms the Device Home was updated. Click **Close** to return to the Device Home page.

Delete a Device Home

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Device Home**.

The Device Home page is shown.

ADMIN | EVIDENCE | CASES | INVENTORY | REPORTS | HELP

SCHUER, DAVID (DS101) | Last login 13 Feb 2019 | [SIGN OUT]

AGENCY PROFILE | AGENCY SINGLE SIGN-ON | CONFIGURE PROVISIONING | PARTNER AGENCIES | RETENTION CATEGORIES | FIELD VALIDATION

ROLES & PERMISSIONS | RANKS | CITIZEN SETTINGS | **DEVICE HOME** | MANAGED METADATA | TRANSCRIPTION SETTINGS

Device Home


Device Home is provided to help with device inventory management. When device homes are created they will be visible within device search and on individual device profiles.


DEVICE HOME MANAGEMENT

CREATE DEVICE HOMES
Create and manage Device Homes for your agency.

NEW DEVICE HOME

DEVICE HOME NAME	POINT OF CONTACT
12th Precinct	Shoe, Dave (98146)

2. Find the Device Home you want to delete and click the delete icon () on the same line.
3. The next action depends on if the Device Home has any devices assigned.
 - If the Device Home does not have any devices assigned, the system asks you to confirm the deletion.

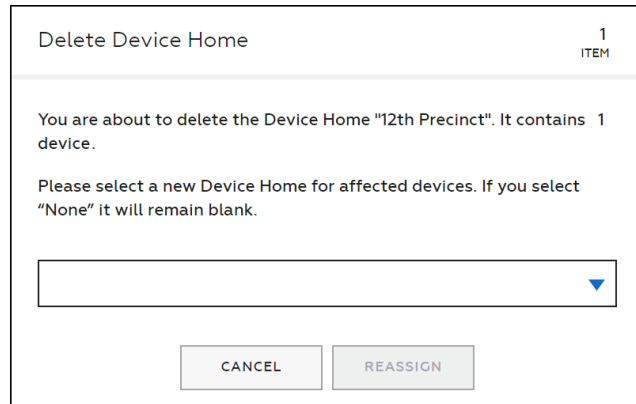


Are you sure you want to delete this home?

CANCEL **DELETE**

Click **Delete**. The system confirms the Device Home was deleted. Click **Close** to return to the Device Home page.

- If the Device Home has devices assigned, the Delete Device Home dialog box is shown.

A dialog box titled "Delete Device Home" with a sub-header "1 ITEM". The main text reads: "You are about to delete the Device Home '12th Precinct'. It contains 1 device." Below this, it says: "Please select a new Device Home for affected devices. If you select 'None' it will remain blank." There is a dropdown menu with a blue arrow icon. At the bottom are two buttons: "CANCEL" and "REASSIGN".

Delete Device Home 1 ITEM

You are about to delete the Device Home "12th Precinct". It contains 1 device.

Please select a new Device Home for affected devices. If you select "None" it will remain blank.

CANCEL REASSIGN

Select the new Device Home for all devices that are assigned to the Device Home you want to delete. You can select **None** to leave the Device Home blank for the Devices.

Click **Reassign**. The system confirms the Device Home was deleted. Click **Close** to return to the Device Home page.

Custom Metadata

The Custom Metadata feature allows your agency to configure additional custom metadata fields that can be associated with evidence. This feature allows you to customize the metadata associated with evidence in order to capture all the information required by your agency.

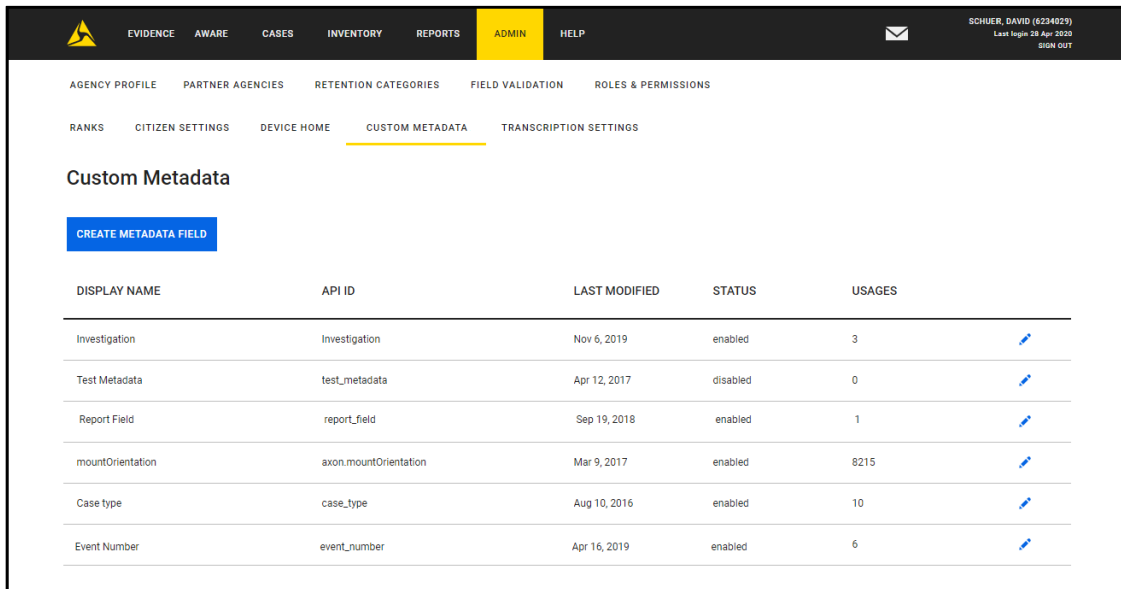
The feature supports three types of custom metadata fields:

- Freeform – This is a free-form text entry field.
- Validated – This is a free-form entry text field, but the entry must conform to the Regular Expression (Regex) definition for the field. This field type can include a description to help users properly enter information.
- Drop-down - The user is presented with a list and selects information.

Viewing Information about Custom Metadata

To view information about managed metadata fields configured for your Evidence.com agency, on the menu bar, click **Admin** and then under Agency Settings, click **Custom Metadata**.

The Custom Metadata page lists all managed metadata fields configured for your agency, regardless of whether the fields are enabled or disabled.



DISPLAY NAME	API ID	LAST MODIFIED	STATUS	USAGES
Investigation	Investigation	Nov 6, 2019	enabled	3
Test Metadata	test_metadata	Apr 12, 2017	disabled	0
Report Field	report_field	Sep 19, 2018	enabled	1
mountOrientation	axon.mountOrientation	Mar 9, 2017	enabled	8215
Case type	case_type	Aug 10, 2016	enabled	10
Event Number	event_number	Apr 16, 2019	enabled	6

- **Display Name** — The text is shown to users when they are selected a custom metadata field on the Evidence Detail page. Valid values are case-sensitive alphanumeric characters and spaces, without punctuation.
- **API ID** — The name that the Evidence.com partner API uses to refer to the managed metadata field. This field name must be unique. Valid values are case-sensitive alphanumeric characters and the underscore character. Other punctuation and spaces are supported. When creating a metadata field, the Unique Field ID is used as the API ID.
- **Last Modified** — The date of the most recent change to the metadata field.
- **Status** — Whether the field is enabled or disabled. An enabled metadata field can be added on the Evidence Detail page and may be available as a filter on evidence search pages in Evidence.com.

If a field is disabled, it only appears on the Evidence Detail page if it was given a value before it was disabled; otherwise, a disabled field does not appear on the Evidence Detail page. A disabled field is never available as a filter on evidence search pages.

- **Usages** — The number of evidence files for which the metadata field has a value, that is, is not empty. For example, if users configured values for a particular metadata field on 50 evidence files, the Usages column would display "50".

Create a Custom Metadata Field

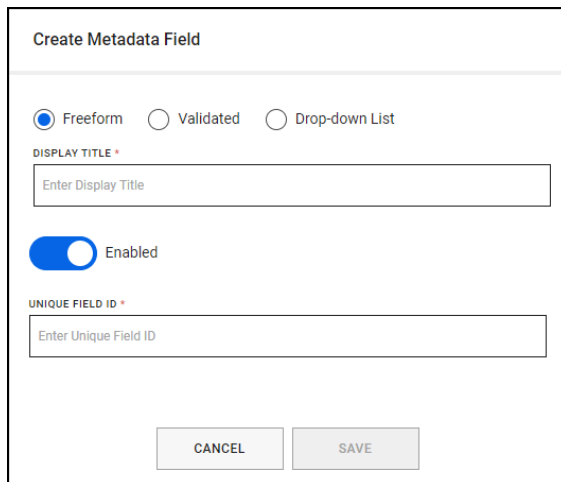
In order to enable users to apply custom metadata to evidence in your Evidence.com agency, you create custom metadata fields.

4. On the menu bar, click **Admin** and then under Agency Settings, click **Custom Metadata**.

The Custom Metadata page lists all custom metadata fields configured for your agency, regardless of whether the fields are enabled or disabled.

5. Click **Create Metadata Field**.

A dialog box for creating a metadata field appears.

A screenshot of the 'Create Metadata Field' dialog box. At the top, the title 'Create Metadata Field' is displayed. Below the title are three radio buttons: 'Freeform' (selected), 'Validated', and 'Drop-down List'. Underneath is a text input field labeled 'DISPLAY TITLE *' with the placeholder text 'Enter Display Title'. Below this is a toggle switch labeled 'Enabled', which is currently turned on. Underneath the toggle is another text input field labeled 'UNIQUE FIELD ID *' with the placeholder text 'Enter Unique Field ID'. At the bottom of the dialog are two buttons: 'CANCEL' and 'SAVE'.

6. Select the type of field you want to create- Freeform, Validated, or Drop-down List.
7. In the **Display Name** field, type the name that you want to assign to the metadata field.

The Unique Field ID is automatically filled in as you enter the name.

8. By default, the Enabled option is selected. If you do *not* want users to have access to the field you are creating, click the toggle to disable the field.
9. Optionally, you can modify Unique Field ID value. The Unique Field ID value is used in the Evidence.com partner API uses to refer to the custom metadata field.
10. If you are creating a Validated field:
 - In the **Regex** field, 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 **Description** field, enter the text that you want to appear as hint text in field.
11. If you are creating a Drop-down List field, under Drop-Down Items:
 - Enter the text for the first option.
 - Enter the text for the second option.
 - If needed, click **Add another list item** and enter the text for the option. Repeat as needed until all the options are added.
 12. Click **Save**.

Evidence.com adds the new metadata field to the bottom of the list of custom metadata fields.

Editing a Custom Metadata Field

You can take the following actions on an existing metadata field:

- **Disable** — You can disable a field that is currently enabled. When a field is disabled, it only appears on the Evidence Detail page if it was given a value before it was disabled; otherwise, a disabled field does not appear on the Evidence Detail page. A disabled field is never available as a filter on evidence search pages.

In order to ensure that managed metadata is never lost, you *cannot* delete a metadata field.

- **Enable** — You can enable a field that is currently disabled. When a field is enabled, it appears on the Evidence Detail page and may be available as a filter on evidence search pages in Evidence.com.
- **Rename** — You can change the display name associated with a custom metadata field.
- **Edit Validation** – For Validated fields, you can change the Regex validation and description text.
- **Edit Options** – For Drop-down lists, you can add or hide selection options. You cannot delete a selection option; you can only hide it.

1. On the menu bar, click **Admin** and then under Agency Settings, click **Custom Metadata**.

The Custom Metadata page lists all managed metadata fields configured for your agency, regardless of whether the fields are enabled or disabled.

2. In the list, find the metadata field you want to edit.
3. Click the edit icon (✎) at the end of the row.

A dialog box for editing the metadata field appears.

4. Edit the field as needed. You can:
 - Click the Enabled toggle to enable or disable the field.
 - Enter a new display name in the Display Name field
 - For Validated fields, enter a new Regex validation and/or description text.
 - For Drop-down lists, you can hide selection options using the toggle. You cannot delete a selection option; you can only hide it.
 - For Drop-down lists, you can add a selection options by clicking **Add another list item** and entering the text for the option. Repeat as needed until all the options are added.
5. Click **Save**.

In the list of metadata fields, the field you updated shows the changes that you made.

Human 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.

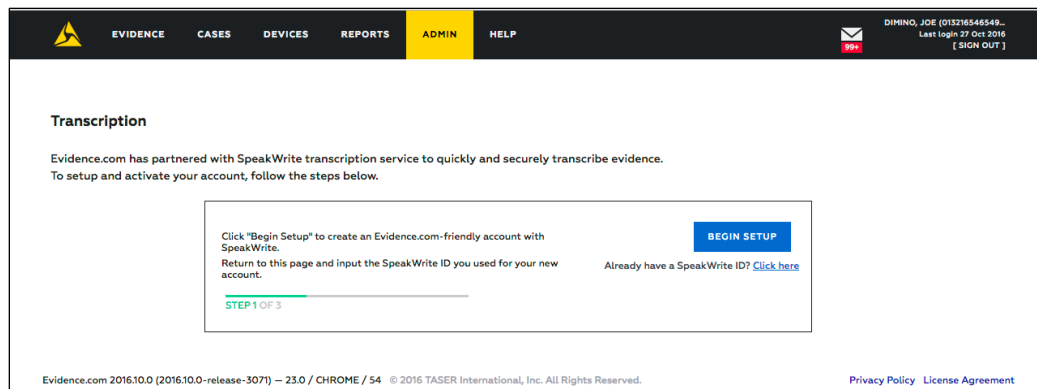
Note: This service is currently only available for customers in the United States, but will be expanding to other regions in the future.

Human 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 **Human Transcription**.

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 SpeakWrite 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**.



Complete this form to Sign-Up and link SpeakWrite to your Evidence.com accounts

A representative will contact you regarding the functionality of your account, setup of billing and final connection to SpeakWrite's 24/7/365 On-Demand transcription service.

Customer Information

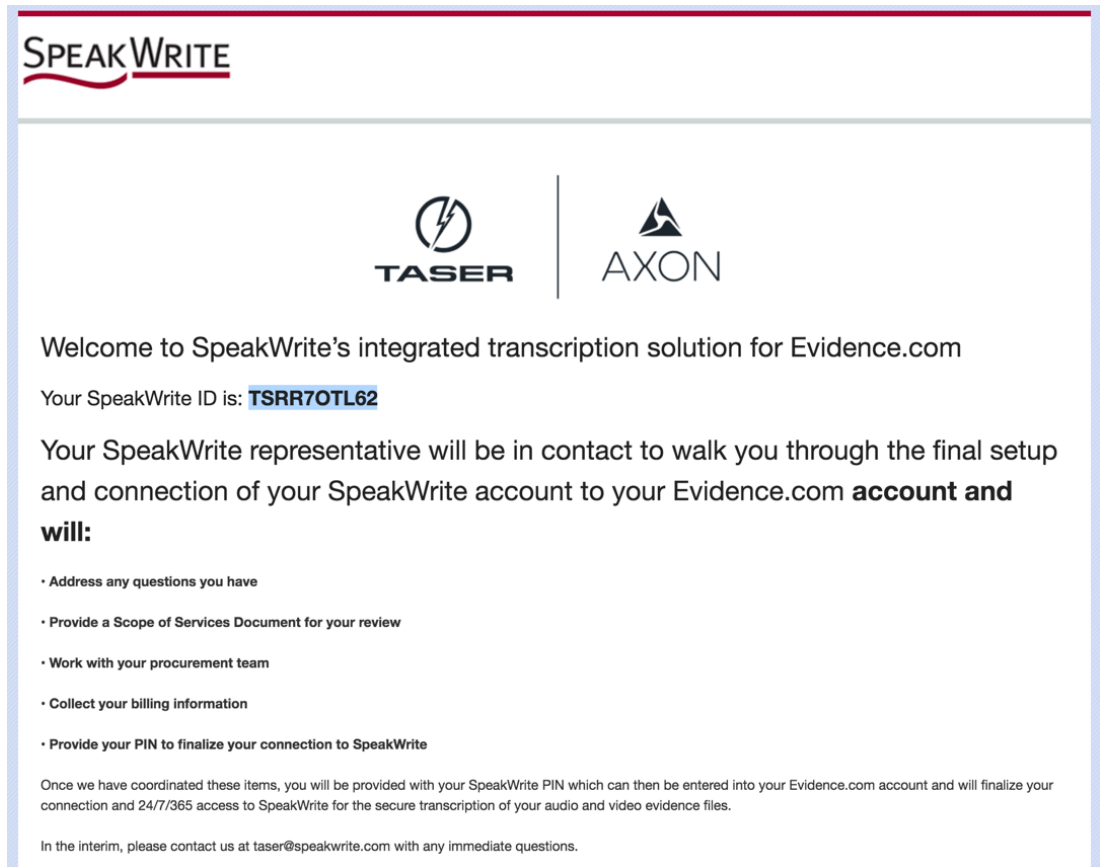
Phone Number: (10 Digits Only) ♦	First Name ♦	Last Name ♦
<input type="text" value="null"/>	<input type="text" value="null"/>	<input type="text" value="null"/>
Email ♦	Company / Department ♦	
<input type="text" value="null"/>	<input type="text" value="null"/>	

Create an Account

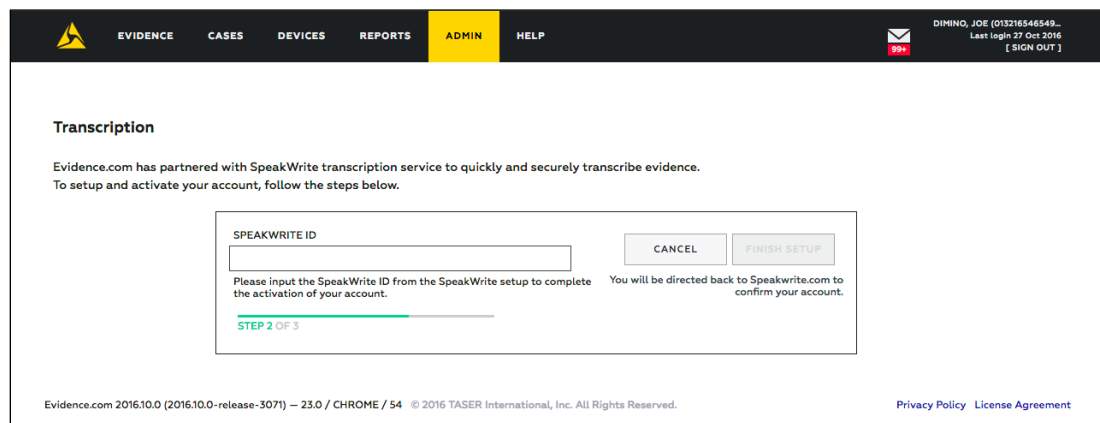
Questions? Please contact us at taser@speakwrite.com and a representative will follow-up with you.

© 1997-2016 all rights reserved

5. Copy your SpeakWrite ID.



6. Return to the Evidence.com browser tab, enter or paste your SpeakWrite ID, and then click **Finish Setup**.



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.

Redaction Settings

The Redaction Settings page is used to add, enable/disable, and delete redaction disclaimers. Redaction disclaimers are a way for your agency to provide information and context to viewers about the content of the redacted videos.

Redaction disclaimers are added to the beginning of redacted videos in Redaction Studio.

Create a Redaction Disclaimer

1. On the menu bar, click **Admin** and then under Agency Settings, click **Redaction Settings**.
2. On the Redaction Settings page, click **Add Disclaimer**.
3. Enter the following disclaimer information:

The screenshot shows the 'Add Redaction Disclaimer' form in the Axon Evidence interface. The form is located under the 'ADMIN' tab, specifically in the 'REDACTION SETTINGS' section. The form fields include:

- NAME ***: A text input field containing 'Disturbing Content'.
- Agency Logo**: A checkbox that is checked, indicating the agency logo should be used.
- TITLE**: A text input field containing 'Disturbing Content'.
- CONTENT**: A text area containing placeholder text: 'Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam faucibus maximus lobortis. Aenean hendrerit, purus in malesuada luctus, turpis dui rhoncus elit, a venenatis felis lacus nec diam. Integer diam enim, auctor et auctor nec, tempor eu ipsum. Vivamus tempor augue ac nisi dictum, eu laoreet tortor ornare.'
- DURATION (SECONDS) ***: A text input field containing '10'.
- Enable Disclaimer**: A toggle switch that is currently turned on.
- CANCEL** and **SAVE** buttons.

Below the form, there is a preview of the disclaimer as it will appear in a video. The preview shows a dark background with a blue shield logo containing a white star and the text 'LOGO NAME'. Below the logo, the text 'Disturbing Content' is displayed, followed by the same placeholder text as in the content field.

At the bottom of the form, there is a note: 'After saving, disclaimer cannot be edited. Please check carefully.'


- Add the disclaimer Name. The name is shown to Redaction Studio users when they are selecting a disclaimer. It is not shown in the redacted video.
- Select the agency logo from your Agency Profile is shown in the disclaimer.
- Add a Title, which is shown below the logo and above the Content. Recommended Title length, including spaces, is 100 characters.

- Add Content explaining the disclaimer. Recommended Content character length, including spaces, is 1,300 characters if the title is not present, and 1,000 characters if the title is present.
 - Set how long the disclaimer is shown before starting the video. This can be 1 to 60 seconds.
 - Select if the disclaimer should be enabled when it is saved. Disclaimers can be enabled and disabled after the disclaimer is saved.
4. Click **Save** to save the disclaimer.

Enable and Disable Redaction Disclaimers

1. On the menu bar, click **Admin** and then under Agency Settings, click **Redaction Settings**.
2. On the Redaction Settings page, find the Redaction Disclaimer you want to enable or disable.
3. Toggle the status switch.

Delete Redaction Disclaimers

1. On the menu bar, click **Admin** and then under Agency Settings, click **Redaction Settings**.
2. On the Redaction Settings page, find the Redaction Disclaimer you want to delete.
3. Click the  (delete) icon.

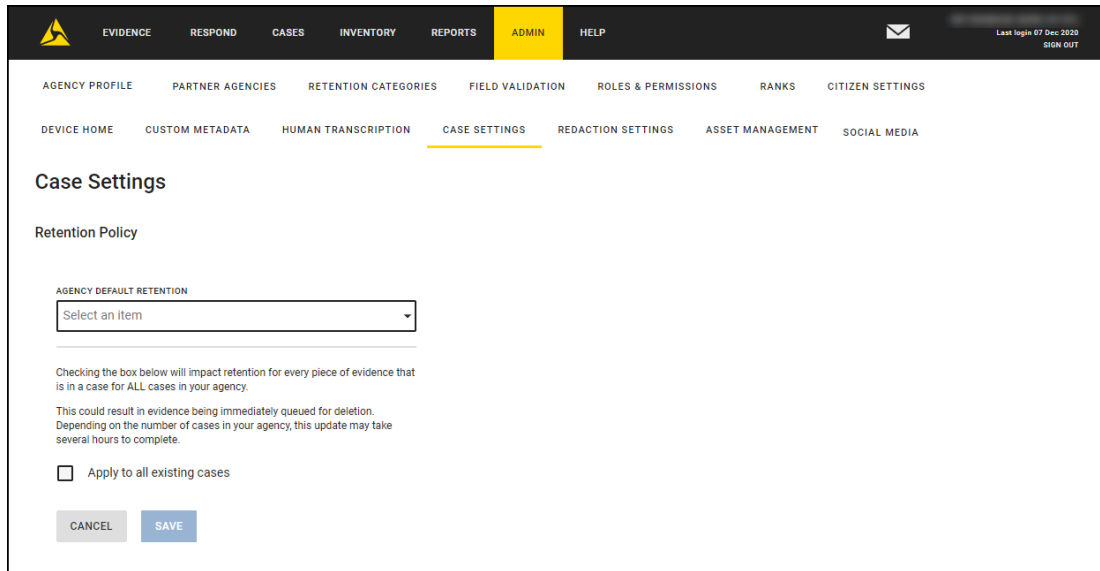
The system asks you to confirm the deletion. Click **Delete** to confirm.

Case Settings

The Case Settings page allows agency administrators to configure a default retention policy for the agency. The default retention is automatically applied to all newly created cases. Administrators can choose to apply the new default retention policy to all existing cases. However, this could result in evidence being immediately queued for deletion.

4. On the menu bar, click **Admin** and then under Agency Settings, click **Case Settings**.

5. Under Retention Policy, click **Edit**.



The screenshot shows the Axon Evidence web interface. The top navigation bar includes links for EVIDENCE, RESPOND, CASES, INVENTORY, REPORTS, ADMIN (highlighted in yellow), and HELP. A user profile icon and 'Last login 07 Dec 2020 SIGN OUT' are on the right. Below the navigation bar, a sub-menu shows various settings categories, with 'CASE SETTINGS' highlighted. The main content area is titled 'Case Settings' and contains a 'Retention Policy' section. This section features a dropdown menu labeled 'AGENCY DEFAULT RETENTION' with the text 'Select an item'. Below the dropdown, a warning message states: 'Checking the box below will impact retention for every piece of evidence that is in a case for ALL cases in your agency. This could result in evidence being immediately queued for deletion. Depending on the number of cases in your agency, this update may take several hours to complete.' There is a checkbox labeled 'Apply to all existing cases' which is currently unchecked. At the bottom of the section are 'CANCEL' and 'SAVE' buttons.

6. Select the Agency Default Retention.

There are three retention policy options:

- **Until Manually Deleted:** This option maintains functional parity with the current system case retention and supports the ability to retain all evidence in cases forever. This is every agency's default retention policy until updated by an agency administrator.
- **Longest Retention Period:** The scheduled deletion date for the case is calculated by finding the longest duration category applied to evidence in the case and adding it to the most recent Recorded On date for any evidence in the case.
- **Individual Evidence Retention:** The case does not impact retention and each piece of evidence in the case is retained based on its own assigned categories and Recorded On date.

Note: Evidence in multiple cases will use the longest retention policy for the cases.

7. Optionally, select you want the new policy to **Apply to all existing cases**.

IMPORTANT: Selecting this option could result in evidence being queued for deletion. Additionally, depending on the number of cases at your agency, it may take several hours to complete the update.

8. Click **Save**.

Devices and Applications Settings

Under Devices on the Admin portal page, administrators can access settings for the following features:

- Body Camera
 - Axon Body 3
 - Axon Body 2 & Flex 2
 - Axon Body & Flex
 - Early Access Devices
- Fleet
 - Axon Fleet 1 & 2
 - Axon Fleet 3
 - Wireless Offload Servers
- CEW
 - TASER 7
 - TASER 7 CQ
 - TASER X2 & X26P
- Signal
 - Signal Vehicle Configuration
 - Fleet 3 Hub Configuration
 - CEW Configuration
 - Signal Sidearm Configuration and Registration
- Applications
 - Evidence Upload XT
 - Axon View
 - Axon Capture

Configure Body Camera Settings

The Body Camera Settings section enables agency administrators to control settings for Axon body worn cameras – such as video quality, event pre-buffering, audio mute control, and indicator light control. It also allows administrators to add devices as Early Access Devices. There are separate pages for controlling the settings for an agency's Axon Body 3 cameras, Axon Body 2 and Axon Flex 2 cameras, and Axon Body and Axon Flex cameras.

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 Devices and Applications – Body Camera click the appropriate body camera link.

There are separate Body Camera setting pages for Axon Body 3 cameras, Axon Body 2 and Flex 2 cameras, and Axon Body and Flex 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.

Early Access Devices

Early Access Devices are an optional way for an agency to set up Axon Body 3 cameras, 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.

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 Devices and Applications, click **Early Access Devices**.
2. Find the type of device (Axon Body 3, Axon Body 2, Axon Dock, Axon Flex 2, or Axon Flex 2 Controller) you want to add.



Early Access Devices

Early Access devices will receive firmware updates before general release in order to allow adequate testing of the changes. If, in testing, your agency finds an issue with the updated devices, please contact Customer Support.



AXON BODY 2


Enter the serial numbers for Axon Body 2 only. You may add up to 15 devices.

SERIAL NUMBER	ASSIGNEE	FIRMWARE VERSION	
X81219479	 Joshua Jones	114.12	

ADD DEVICE

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 **Devices and Applications**, 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.

Body Camera Wi-Fi Networks

The Automatic Wi-Fi Upload feature enables cameras to automatically upload evidence over Wi-Fi when in proximity to a pre-configured network. The Automatic Wi-Fi Upload feature is available for all Axon Body 3 customers and is not dependent on any unique licenses.

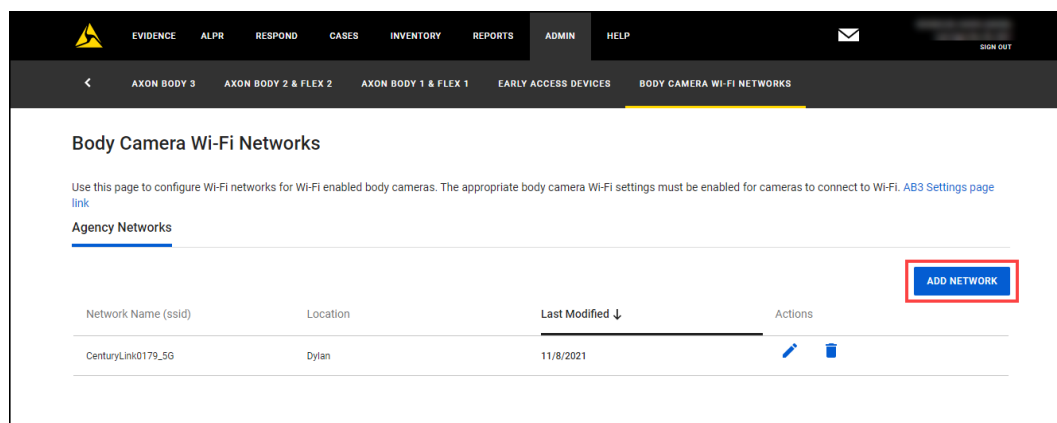
Agency Axon Evidence administrators can enable the Automatic Wi-Fi Upload feature and workflow by setting up authorized Wi-Fi access points and then enabling the Axon Body 3 Automatic Wi-Fi Upload setting.

The Body Camera Networks page is used to pre-configure WPA2 Personal Wi-Fi networks. While WPA2-TKIP, WPA, and WEP are technically supported, Axon recommends using WPA2-PSK networks.

All agency Axon Body 3 cameras need to be docked to download any additions, modifications, or deletions to the network list on the Body Camera Wi-Fi Networks page.

Adding a Body Camera Wi-Fi Network

1. On the menu bar click **Admin** and then click **Body Camera Wi-Fi Networks**.
2. Click **Add Network**. The Add Network screen is shown on the right side of the page.



3. Enter the Network Name (SSID) and Password for the network. Axon recommends using WPA2-PSK networks for increased security measures. Optionally, you can add Location information to differentiate networks with similar names.

The screenshot shows the 'Add Network' dialog box on the right side of the screen. The dialog has a title bar with a close button. It contains three sections: 'Credentials' with fields for 'NETWORK NAME (SSID) *' and 'PASSWORD *', and 'Notes' with a 'LOCATION' field. There are 'CANCEL' and 'SAVE' buttons at the bottom. The background shows the 'Body Camera Wi-Fi Networks' page with a table of networks.

Network Name (ssid)	Location	Last Modified ↓	Action
CenturyLink0179_5G	Dylan	11/8/2021	

4. Click **Save**.

Add more networks as needed. Once all the network information is saved, you can go back and modify existing networks or delete existing networks.

Editing a Body Camera Wi-Fi Network

1. On the menu bar click **Admin** and then click **Body Camera Wi-Fi Networks**.
2. Find the network you want to edit and the click (edit network) icon. The Edit Network screen is shown on the right side of the page.
3. Edit the Network Name (SSID), Password, and Location information as needed.
4. Click **Save**.

Deleting a Body Camera Wi-Fi Network

1. On the menu bar click **Admin** and then click **Body Camera Wi-Fi Networks**.
2. Find the network you want to delete and the click (delete network) icon.
3. The asks you to confirm you want to delete the network. Click **Delete** to delete the network.

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 and Applications - Fleet, click the appropriate Axon Fleet link.

There are separate settings for Axon Fleet 3 and Axon Fleet 1 & 2.

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 Settings, see the [Fleet 3 Settings](#) or [Fleet 1 & 2 Settings](#) in Appendix C.

3. At the bottom of the page, click **Save Settings**.

Axon Evidence saves the camera settings. When View XL (Fleet 1 & 2) or the Fleet Dashboard (Fleet 3) is connected to Axon Evidence, it automatically checks for and applies any updated configuration settings every 10 minutes.

Configure CEW Settings

The CEW Settings page enables administrators to configure Conducted Energy Weapons (CEW) Settings based on agency policy. There are separate setting pages for TASER 7 and TASER X2 & X26P CEWs.

TASER 7 Settings

1. On the menu bar, click **Admin** and then under Devices and Applications - CEW, click **TASER 7**.

The TASER 7 Settings page appears.

TASER 7 Settings

Laser

The TASER 7 uses two lasers to identify approximate impact location of the top and bottom cartridge probes.

☐ On - Both Lasers Solid
☐ On - Top Laser Solid, Bottom Laser Blinking
☒ Off

Flashlight Power

☒ High
☐ Low
☐ Off

Automatic Shut-Down

When set to Hard Stop, the CEW automatically shuts-down electrical discharge after 5 seconds, regardless of if the trigger or arc switch is being held down. When set to Arc Switch Override, the CEW continues electrical discharge after 5 seconds, as long as the arc switch is being held down. When set to Disabled, the CEW continues electrical discharge after 5 seconds, as long as the trigger and/or arc switch is being held down.

☐ Enabled - Hard Stop
☐ Enabled - Arc Switch Override
☒ Disabled

Tilt Select

The Tilt Select feature allows users to switch the active bay that will be deployed when the trigger is pulled. If this feature is activated, the user will see the active cartridge underlined on the CID of the device. A quick sideways tilt of the device will change bays. Note that this is an intentional motion that uses the device's accelerometer to determine if the TASER has been tilted >45 degrees and returned to upright in under one second. Further details on this motion and a video demonstrating the capability can be found by searching "Tilt Select" on my.axon.com. This feature will be available starting with Firmware version 1.6 (May 2020).

If both Close-Quarters and Stand-Off cartridges are inserted in the TASER, the lasers will automatically change to represent the angle of the cartridge in the active bay. If "Enabled - Training Only" is selected, the user may only take advantage of this feature when Inert or HALT cartridges are inserted. This particular setting lets users test the feature to see if they would like to activate it for live cartridges in the field.

☐ Enabled - All Cartridge Types
☒ Enabled - Training Only
☐ Disabled

Cartridge Deployment in Function Test Mode

Determines if TASER 7 automatically exits Function Test Mode and deploys a cartridge when the trigger is pulled. When disabled, a trigger pull in Function Test Mode only begins an arc activation across bays 1 and 2 for approximately 5 seconds. This is the same functionality as pressing the arc switch in Function Test Mode. When disabled, to manually exit Function Test Mode, shift the safety switch down (SAFE) and then up (ARMED) to power off the TASER, exit Function Test Mode, and power on in Weapons Mode. Note: this setting can only be disabled in FW versions 1.9.0 and above.

☒ Enabled
☐ Disabled

2. As needed, configure the **LASER**, **Flashlight Power**, **Automatic Shut-Down**, **Tilt Select** and **Cartridge Deployment in Function Test Mode** settings.

3. Click **Save**.

Evidence.com saves the TASER 7 settings. The settings are applied to TASER battery packs when the packs are placed in TASER 7 Docks for charging.

TASER 7 CQ Settings

1. On the menu bar, click **Admin** and then under Devices and Applications-CEW, click **TASER 7 CQ**.

The TASER 7 CQ Settings page appears.

TASER 7 CQ Settings

Laser
The TASER 7 CQ uses a single laser to identify approximate impact location of the top and bottom cartridge probes.

☒ On
☐ Off

Flashlight Power

☐ High
☒ Low
☐ Off

Automatic Shut-Down
When set to Hard Stop, the CEW automatically shuts-down electrical discharge after 5 seconds, regardless of if the trigger or arc switch is being held down. When set to Arc Switch Override, the CEW continues electrical discharge after 5 seconds, as long as the arc switch is being held down. When set to Disabled, the CEW continues electrical discharge after 5 seconds, as long as the trigger and/or arc switch is being held down.

☐ Enabled - Hard Stop
☒ Enabled - Arc Switch Override
☐ Disabled

Cartridge Deployment in Function Test Mode
Determines if TASER 7 automatically exits Function Test Mode and deploys a cartridge when the trigger is pulled. When disabled, a trigger pull in Function Test Mode only begins an arc activation across bays 1 and 2 for approximately 5 seconds. This is the same functionality as pressing the arc switch in Function Test Mode. When disabled, to manually exit Function Test Mode, shift the safety switch down (SAFE) and then up (ARMED) to power off the TASER, exit Function Test Mode, and power on in Weapons Mode. Note: this setting can only be disabled in FW versions 1.9.0 and above.

☒ Enabled
☐ Disabled

SAVE

2. As needed, configure the **LASER**, **Flashlight Power**, **Automatic Shut-Down** and **Cartridge Deployment in Function Test Mode** settings.

3. Click **Save**.

Evidence.com saves the TASER 7 CQ settings. The settings are applied to TASER battery packs when the packs are placed in TASER 7 Docks for charging.

TASER X2 & X26P Settings

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 and Applications-CEW, click **TASER X2 & X26P**.

The X2 & X26P Settings page appears.

The screenshot shows the 'X2 and X26P Settings' page. At the top, it states: 'The CEW settings shown here are the default agency settings and affect the specific CEW devices.' Below this, a note says: 'These settings affect both the APPM and SPPM. To disable the automatic shut-down capabilities on the SPPM check the disable box.' There are three radio button options: 'Arc Switch Override', 'Hard Stop' (selected), and 'Disable SPPM Automatic Shut-Down (includes X26P)' (checked with a blue checkmark). Under 'FIRING MODE SETTING', there are two radio button options: 'Semi-Automatic' (selected) and 'Manual'. Under 'CONTINUED SPPM TRANSMIT IN SAFE SETTING', a note explains: 'This setting affects CEWs with the SPPM. When enabled, the CEW remains powered and Axon Signal finishes the normal 30-second transmission when the safety is placed in the SAFE position.' Below this, an important note states: 'Important: Selecting enable decreases expected battery lifetime firings.' There are two radio button options: 'Enable: CEW Remains On And Continues Signal Transmission In Safe' and 'Disable: CEW Turns Off And Discontinues Signal Transmission In Safe' (selected). Under 'ADDITIONAL SETTINGS', there are two checkboxes: 'Laser Setting Off for 35' Cartridges' (checked) and 'Share engineering logs with Axon to help improve product security and functionality' (unchecked). At the bottom left, there is a blue 'SAVE' button.

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 3, 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 1 and Fleet 2 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 2 front camera when a vehicle's light bar is turned on. When vehicle A turns on its light bar, the Fleet 2 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.

Note: In the August 2019 release, the Evidence Audit Trails and Device Audit Trails were updated to specifically reflect the Signal Input pin number on the Axon Signal Vehicle that initiated an Axon Fleet camera activation signal. In situations where two inputs were active at the time of camera activation, both Axon Signal input pins are included in the audit trail entry.

1. On the menu bar, click **Admin** and then, under Signal, click **Signal Vehicle**.

<div>  <div> EVIDENCERESPONDCASESINVENTORYREPORTSADMINHELP </div> <div>  <div> <div></div> <div>SIGN OUT</div> </div> </div> </div>																																																	
<div> SIGNAL VEHICLEFLEET 3 HUBCEWSIGNAL SIDEARM </div>																																																	
<h3>Signal Vehicle</h3> <p>These settings determine which 12V inputs activate Body Worn, Fleet 1, and Fleet 2 cameras.</p> <table> <tr> <th>INPUT</th><th>LABEL</th><th>RULE</th><th>CAMERAS</th><th></th></tr> <tr> <td>5</td><td>Front Door Driver Side</td><td>Activate</td><td>Body Worn</td><td></td></tr> <tr> <td>6</td><td>Light Bar</td><td>Activate</td><td>Body Worn</td><td></td></tr> <tr> <td>7</td><td>Rear Doors</td><td>-</td><td>-</td><td></td></tr> <tr> <td>8</td><td>K9 Door</td><td>Activate</td><td>Body Worn, Fleet 1 & 2 Interior, Fleet 1 & 2 Front</td><td></td></tr> <tr> <td>9†</td><td>Light Bar Code 1</td><td>Activate; 5s delay</td><td>Body Worn, Fleet 1 & 2 Interior, Fleet 1 & 2 Front</td><td></td></tr> <tr> <td>10†</td><td>Light Bar Code 2</td><td>Activate; No delay</td><td>Fleet 1 & 2 Front</td><td></td></tr> <tr> <td>11†</td><td>Light Bar Code 3</td><td>Activate; No delay</td><td>Body Worn, Fleet 1 & 2 Front</td><td></td></tr> <tr> <td>12†</td><td>-</td><td>-</td><td>-</td><td></td></tr> </table> <p>† Signal Vehicle inputs 9, 10, 11, & 12 support activation delays. Signal Vehicle unit and Body Cameras require supporting firmware. Fleet 1 & 2 cameras do not support delays. See the Axon product guides on Signal Configuration for more information.</p>					INPUT	LABEL	RULE	CAMERAS		5	Front Door Driver Side	Activate	Body Worn		6	Light Bar	Activate	Body Worn		7	Rear Doors	-	-		8	K9 Door	Activate	Body Worn, Fleet 1 & 2 Interior, Fleet 1 & 2 Front		9†	Light Bar Code 1	Activate; 5s delay	Body Worn, Fleet 1 & 2 Interior, Fleet 1 & 2 Front		10†	Light Bar Code 2	Activate; No delay	Fleet 1 & 2 Front		11†	Light Bar Code 3	Activate; No delay	Body Worn, Fleet 1 & 2 Front		12†	-	-	-	
INPUT	LABEL	RULE	CAMERAS																																														
5	Front Door Driver Side	Activate	Body Worn																																														
6	Light Bar	Activate	Body Worn																																														
7	Rear Doors	-	-																																														
8	K9 Door	Activate	Body Worn, Fleet 1 & 2 Interior, Fleet 1 & 2 Front																																														
9†	Light Bar Code 1	Activate; 5s delay	Body Worn, Fleet 1 & 2 Interior, Fleet 1 & 2 Front																																														
10†	Light Bar Code 2	Activate; No delay	Fleet 1 & 2 Front																																														
11†	Light Bar Code 3	Activate; No delay	Body Worn, Fleet 1 & 2 Front																																														
12†	-	-	-																																														

- For each input that you need to configure, click the  icon on the right side of the page.

Note: The Input column shows the inputs that are available for configuration for Axon Signal Vehicle at your agency and represent the wire connection on the Axon signal Vehicle device. Inputs 1 through 4 are reserved and cannot be configured.

- Select the appropriate Label from the list. This is the trigger that the Axon Signal Vehicle device is wired to in the installation, such as Front Door or Light Bar.
- Select the cameras (Body-Worn, Fleet Front, and Fleet Back cameras) that you want to alert with this trigger.

Note: The Fleet 1 & 2 Front and Back camera settings are only available to agencies that use Axon Fleet.

- Click **Save**.
- Repeat steps 2 – 5 for the remaining inputs.

Configure Fleet Hub Signal Settings











This menu configures Fleet Hub to activate Fleet 3 cameras.

- On the menu bar, click **Admin** and then under Signal, click **Fleet 3**.


This menu configures Fleet Hub to activate Fleet 3 cameras.

Fleet 3 Hub

These settings determine which 12V inputs activate Fleet 3 cameras and log status in the Fleet 3 Hub Audit Trail. Brake, lights, & siren inputs are overlaid during video playback in Axon Evidence.

Input	Label ⓘ	Rule	Camera	
5	-	-	-	
6	-	-	-	
7	-	-	-	
8	-	-	-	
9	-	-	-	
10	-	-	-	
11	-	-	-	
12	-	-	-	
13†	-	-	-	
14†	-	-	-	

† Brakes label can only be configured on inputs 13 and 14

- To configure an input, find the correct row. Click the  (edit) icon at the end of the row.

Brakes are only configurable on inputs 13 and 14.

- Click the dropdown under the Label column. Click the desired Label.

Some labels have a letter in parenthesis. This indicates the letter shown on the metadata overlays when reviewing an associated video in Axon Evidence.

- Click the dropdown under the Rule column. Click the desired behavior.

Log status will log the action in the audit trail, while activate will activate the selected cameras.

- If the selected Rule includes activation, click the dropdown in the Camera column. Select cameras to activate.

- When you have finished configuring an input click **Save**.

- To configure another Fleet Hub input, repeat steps 2 – 6.

Once all edits are completed, you can go to any other Axon Evidence page.

Configure CEW Signal Settings


1. On the menu bar, click **Admin** and then, under Signal, click **CEW**.

CEW

CEW ACTIVATIONS	CAMERA ACTIVATIONS
Armed	Front, Body Worn, Back
Arc	Body Worn
Trigger	

Assigned Officer Activation
 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.

☐ Disabled

2. Click the  icon to the right of the **CEW Activation** you want to set.
 3. Select the cameras (Body-Worn, Fleet Front, and Fleet Back cameras) that you want to alert with this CEW activation.
- Note:** The Fleet 1 & 2 Front and Back camera settings are only available to agencies that use Axon Fleet.
4. Click **Save**.
 5. Repeat steps 2 – 4 for the remaining CEW activations.
 6. Optionally, move the Assigned Officer Activation switch as needed 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.

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.

Axon Evidence saves your CEW Activations settings.

Configure Signal Sidearm Settings

1. On the menu bar, click **Admin** and then, under Signal, click **Signal Sidearm**.

Signal Sidearm

SIGNAL SIDEARM ACTIVATIONS	CAMERA ACTIVATIONS
Weapon Drawn	Body Worn, Back, Front

Assigned Officer Activation
When enabled, the Axon Signal transmission from a Signal Sidearm device only activates the Axon body worn camera assigned to the device user. When disabled, the Axon Signal transmission from a Signal Sidearm device activates any in-range Axon body worn camera.

☐ Disabled

Mute Mode Capability
When Mute Mode capability is enabled for your agency, officers can use the Signal Sidearm button to enter Mute Mode. Mute Mode allows officers to remove their firearm from their holster without alerting Axon cameras to record.

☐ Disabled

Signal Sidearm Registration
Axon Device Manager is the preferred method for registering and assigning devices. Use this page to register and assign Signal Sidearm units if you don't have access to Axon Device Manager. Maintaining up-to-date Signal Sidearm and assignee ensures accurate audit trail information and improves firmware update process of the unit.

SERIAL NUMBER:

ASSIGNEE (OPTIONAL):

REGISTER DEVICE

2. Click the icon to the right of **Weapon Drawn**.
3. Select the cameras (Body-Worn, Fleet Front, and Fleet Back cameras) that you want to alert with Signal Sidearm.

Note: The Fleet 1 & 2 Front and Back camera settings are only available to agencies that use Axon Fleet.

4. Click **Save**.

Evidence.com saves your Signal Sidearm Activations settings.

5. Optionally move the Assigned Officer Activation switch as needed enable or disable this capability.

When enabled, the Axon Signal transmission from Signal Sidearm only activates the Axon body worn camera assigned to the user. When disabled, the Axon Signal transmission from Signal Sidearm activates any in-range Axon body worn camera.

IMPORTANT: To ensure the Signal Sidearm Assigned Officer Activation setting functions as designed, your agency must ensure that Signal Sidearm and Axon Body Worn Cameras are correctly assigned and distributed to officers.

6. Optionally, 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.

Axon Evidence saves Signal Sidearm settings.

Signal Sidearm Registration

Note: Axon recommends using the Axon Device Manager app for registering and assigning Axon Signal Sidearm and other Axon devices.

Administrators manually record sensor serial numbers in Axon Evidence 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 Axon Evidence account.
2. On the menu bar, click **Admin** and then, under Signal, click **Signal Sidearm**.
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.

The screenshot shows the 'Signal Sidearm' configuration page in the Axon Evidence interface. The page has a dark header with navigation tabs: EVIDENCE, RESPOND, CASES, INVENTORY, REPORTS, ADMIN, and HELP. Below the header, there are sub-tabs: SIGNAL VEHICLE, FLEET 3 HUB, CEW, and SIGNAL SIDEARM (which is selected). The main content area is titled 'Signal Sidearm' and contains several sections:

- SIGNAL SIDEARM ACTIVATIONS**: A table with one row showing 'Weapon Drawn'.
- CAMERA ACTIVATIONS**: A table with one row showing 'Body Worn, Back, Front'.
- Assigned Officer Activation**: A section with a description and a toggle switch set to 'Disabled'.
- Mute Mode Capability**: A section with a description and a toggle switch set to 'Disabled'.
- Signal Sidearm Registration**: A section with a description and two input fields: 'SERIAL NUMBER' (containing 'X99...') and 'ASSIGNEE (OPTIONAL)' (containing 'Enter name, email address, or badge ID').

At the bottom of the page, there is a blue button labeled 'REGISTER DEVICE'.

4. Click **Register Device**.

Axon Respond Settings

Axon Respond works in conjunction with Axon Body 3 cameras to allow staff with the appropriate permissions to view officer location when recording and activate livestreams from within Axon Evidence.com.

Axon Respond for Devices is controlled and accessed through Evidence.com, but the information for configuring and using is contained in the Axon Respond for Devices Information Guide on the [Axon Product Guides](#).

Evidence Upload XT Settings

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. The Evidence Upload XT settings page allows administrators to configure the bandwidth setting

options for Evidence Upload XT. Note that this feature requires Evidence Upload XT v1.0.12 or later.

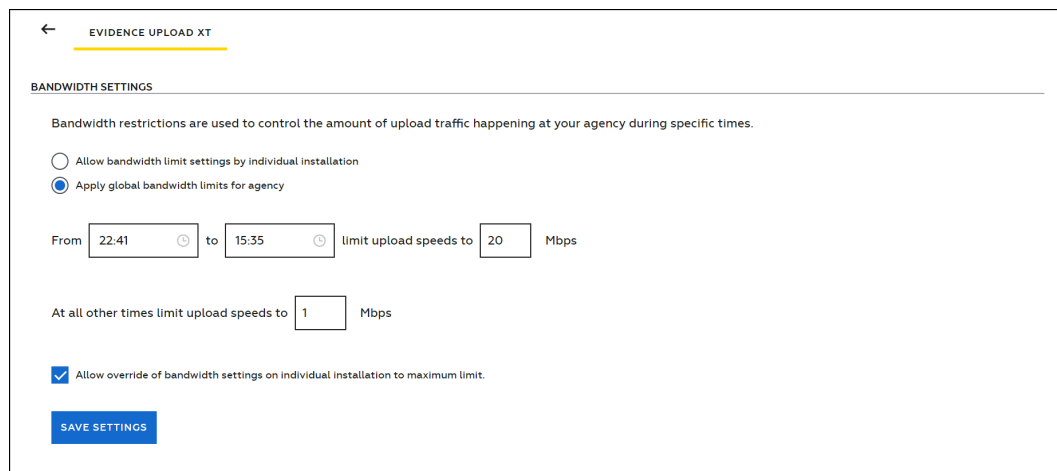
Administrators can select to allow bandwidth limits to be set on individual Evidence Upload XT installations or apply a global bandwidth limit for all Evidence Upload XT installations that connect to the agency. Bandwidth limits can also be managed based on time of day.

If a global bandwidth limit is selected, Evidence Upload XT users will not be able to change the bandwidth setting for their individual installation.

Optionally, administrators can allow individual Evidence Upload XT installations to override the global bandwidth settings during an upload. If this option is enabled, users can select to apply or not apply the bandwidth settings as the last step before they upload files from Evidence Upload XT.

1. Sign in to your Evidence.com account.
2. On the menu bar, click **Admin** and then, under Applications, click **Evidence Upload XT**.
3. On the Bandwidth Settings page, select if you want to **Apply global bandwidth limits** for individual Evidence Upload XT installations for your agency.

If not, skip to step 4. Otherwise:



The screenshot shows the 'EVIDENCE UPLOAD XT' page with a 'BANDWIDTH SETTINGS' section. It includes a description of bandwidth restrictions, two radio button options for limiting upload speeds (individual installation vs. global agency limit), time selection fields (From 22:41 to 15:35), a limit upload speeds field (20 Mbps), and a checkbox for allowing override of bandwidth settings on individual installation to maximum limit. A 'SAVE SETTINGS' button is at the bottom.

- Click the **From** and **to** hour fields to select the hours that bandwidth throttling is active. These settings use a 24-hour clock.
 - Click in the Mbps field and enter the maximum Mbps Evidence Upload XT can use during the set time.
4. If needed, enter the maximum Mbps limit used outside of the global bandwidth limits time for individual Evidence Upload XT installations.

5. Optionally, select **Allow override of bandwidth settings on individual installation to maximum limit**.

If this option is enabled, users can select to apply or override the bandwidth setting limits as the last step before they upload files from Evidence Upload XT.

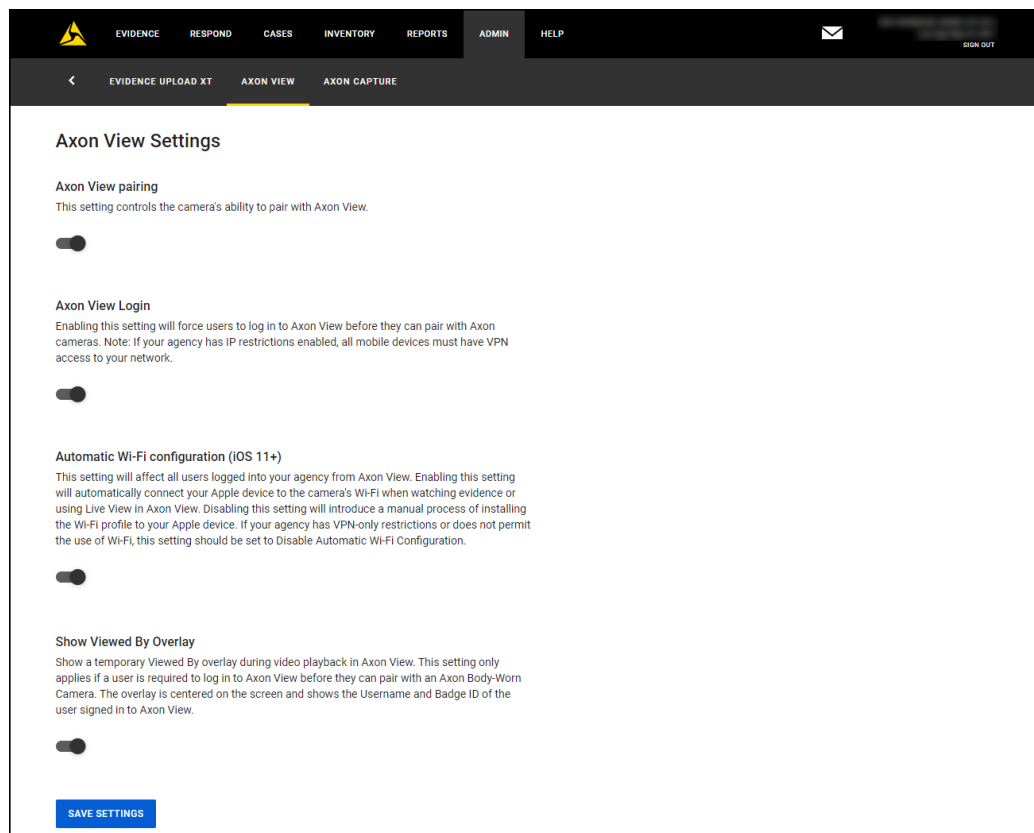
6. Click **Save Settings**.

Axon View Settings

The Axon View Admin settings page provides a central location for maintaining Axon View application settings for your agency.

Important: Axon View for iOS 4.6 or higher is needed to support the Automatic Wi-Fi Configuration functionality.

1. Sign in to your Evidence.com account.
2. On the menu bar, click **Admin** and then, under Applications, click **Axon View**.
3. For each setting, choose the option that best supports your agency's policies for using Axon View.



- **Axon View Pairing** - This sets if the cameras can be paired with the Axon View mobile application.

- **Axon View Login**

Note: Visibility of the Axon View Login setting is managed by an Axon-controlled agency level setting. Agencies that would like to have this setting available can contact their Axon representative or Technical Support to request this option.

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.

- **Automatic Wi-Fi Configuration (iOS)** - This sets if your agency's Apple devices will automatically connect to an Axon Body Camera's Wi-Fi when using the Playback and Live View functions in Axon View. If this setting is disabled, users must manually install the Wi-Fi profile on the Apple device. This setting applies to all iOS devices at your agency that have Axon View installed. Agency Apple devices must have iOS 11 or higher for this option to function correctly.
- **Show Viewed By Overlay** - This sets if a temporary Viewed By overlay is shown during video playback in Axon View. The overlay is centered on the screen and shows the Username and Badge ID of the user signed in to Axon View. This setting only applies if a user is required to log in to Axon View before they pair with an Axon Body-Worn Camera.

Note: This setting currently applies to Axon View for Android v5.4.0 and later. It is currently not available for Axon View for iOS.

4. Click **Save Settings**.

Axon Capture Settings

The Axon Capture Admin settings page provides a central location for maintaining Axon Capture application settings for your agency.

Important: Axon Capture v5.0 or later is needed to support the settings on this page.

1. Sign in to your Evidence.com account.
2. On the menu bar, click **Admin** and then, under Applications, click **Axon Capture**.
3. For each setting, choose the option that best supports your agency's policies for using Axon Capture.

- The Configuration Policy section controls the types of files users can capture and if they can import files from the device's photo/video library.

Important: It can take up to seven days for all devices to be updated to new Configuration Policy settings after the settings are changed and saved in Axon Evidence.com.

- The Watermark Policy section controls whether a permanent watermark is applied to videos captured with the app. The watermark is similar to the one used for Axon body-worn and Fleet cameras. This setting only applies to Axon Capture installed on iOS devices.
- The Deletion Policy section controls if Axon Capture users can manually delete files from the app.

Note: Files that are captured with the app are deleted after upload to Axon Evidence is confirmed.

- The Field Validation Policy section controls if Evidence ID and Category metadata are required when uploading files from the app. Enabling the settings allows users to upload files from Axon Capture without adding an Evidence ID or Category.

Note: If your agency has enabled the agency-wide Evidence ID Field Validation requirement and the Allow Empty Evidence ID setting is disabled, then Axon Capture will enforce the expected format for the Evidence ID.

The screenshot shows the Axon Evidence Admin interface. The top navigation bar includes links for EVIDENCE, CASES, INVENTORY, REPORTS, ADMIN (highlighted), and HELP. The user is SGT SCHUER, DAVID (05101), last login 15 Sep 2019, with a SIGN OUT link. The breadcrumb trail shows EVIDENCE UPLOAD XT, AXON VIEW, and AXON CAPTURE (highlighted). The main heading is "Axon Capture Settings".

Configuration Policy
The following settings affect all users logged into your agency from Axon Capture for iOS and Android.

Allow Photos
This setting controls whether users can capture photos with the app.
☒

Allow Audio
This setting controls whether users can capture audio with the app.
☒

Allow Video
This setting controls whether users can capture video with the app.
☐

Allow Import
This setting controls whether users can import photos and videos from their photo/video library to the app.
☐

Watermark Policy
This setting affects all users logged into your agency from Axon Capture for iOS.

Watermark (iOS Only)
This settings controls whether a permanent watermark appears in the upper right corner of videos captured in the app. The watermark contains the date and time the video file was captured, a notation that the video source is Axon Capture, and the elapsed time for the video.
☐

Deletion Policy
This setting affects all users logged into your agency from Axon Capture for iOS and Android.

Delete Evidence From Capture
This setting controls whether users are allowed to delete evidence captured with the app from the app.
☒

Field Validation Policy
This setting affects all users logged into your agency from Axon Capture for iOS and Android.

Allow Empty Evidence ID
This setting controls whether users are allowed to upload evidence with an empty Evidence ID field.
☐

Allow Empty Category
This setting controls whether users are allowed to upload evidence without adding at least one category.
☐

SAVE SETTINGS

4. Click **Save Settings**.

Security Settings

The Security Settings section allows administrators to: 1) control access to their agency's Axon Evidence account by limiting IP address and apply exceptions for Axon applications, 2)

Configure password requirements for their agency, 3) Configure Multi-Factor Authentication (MFA) settings, and 4) Configure API access clients.

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. Click **Add New IP Address**.
3. Select if you are adding a **Single IP Address** or **Range of IP Addresses**.
4. Enter the IP Address or range of addresses.
5. 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.
6. Click **Add**.

The newly added IP Address shows in the table.

7. You can continue adding additional IP Addresses as needed.
8. Select **Restrict User Access to the Trusted IP Addresses Below** 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.

9. 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 Allowed Lists for Multi-Homed Networks

Evidence.com supports IP security allowed lists for agencies where web traffic can originate from multiple IPs during the same user session. The standard IP allowed list 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 allowed list 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 allowed list 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**.

The IP Active Session Security area appears at the top of the page.

2. Click **Add New IP Address**.
3. Select if you are adding a **Single IP Address** or **Range of IP Addresses**.
4. Enter the IP Address or range of addresses.
5. 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.
6. Click **Add**.

The newly added IP Address shows in the table.

7. You can continue adding additional IP Addresses as needed.
8. Select **Allow IP address to change during an active session to the trusted IP addresses below**.

Axon Application Exceptions

The IP restrictions feature provides additional access security to Axon Evidence.com. However, implementing this feature can impact Axon mobile applications by blocking access, which makes it difficult for officers to effectively use them.

The Axon Application Exceptions settings allow administrators to easily add exceptions to IP restrictions for specific Axon applications.

This feature is only supported on the following Axon mobile application versions:

- Axon Device Manager for iOS v2.0.5 or later
- Axon Device Manager for Android v3.0.4 or later
- Axon View for iOS v5.0.1 or later
- Axon View for Android v5.0.3 or later
- Axon Capture for iOS v5.0 or later
- Axon Capture for Android v5.0 or later
- Axon Aware mobile application for both iOS and Android

Note that previous versions of the Axon mobile applications will continue to function normally, but will be subject to the IP restrictions, if enabled for your agency.

1. On the menu bar, click **Admin** and then under Security Settings, click **IP Address**.

2. Scroll to the bottom of the page to the Axon Application Exceptions section.

The screenshot displays the 'ADMIN' section of the Axon Evidence interface, specifically the 'IP address configuration' page. The top navigation bar includes links for EVIDENCE, RESPOND, CASES, INVENTORY, REPORTS, ADMIN (highlighted), and HELP. A user profile dropdown shows 'Last login: Jan 13, 2021' and a 'SIGN OUT' option.

Below the navigation bar, the 'IP address configuration' section is active. It includes a sub-section for 'IP active session security' with two toggle switches: 'Restrict user access to the trusted IP addresses below' (disabled) and 'Allow IP address to change during an active session to the trusted IP addresses below' (disabled). A button 'ADD NEW IP ADDRESS' is located to the right.

A message states: 'Your current IP address is 73.109.54.93. If you do not add this IP address to the list of allowed IPs, you may lock yourself out of Evidence.com accidentally. If this does happen, you may contact support at evidencehelp@axon.com for assistance.'

A table lists 'Allowed IP addresses' with columns for the IP address and a 'Label'. The table contains three entries:

Allowed IP addresses	Label
55.44.33.22	\`alert("XSS");//
1.2.98.2	test
66.162.141.14	new

Each row has a trash icon for deletion.

The 'Axon application exceptions' section follows, explaining that certain mobility-based Axon applications will be impacted by IP restrictions. It lists several applications with toggle switches to exempt them from IP restrictions:

- Axon View:** Syncs up with Axon cameras to provide instant playback and GPS tagging from a mobile device. Toggle: Exempt this application from IP restrictions (disabled).
- Axon Capture:** Records evidence, uploads data, and more with a smartphone app. Toggle: Exempt this application from IP restrictions (disabled).
- Axon Device Manager:** Allows armorers to manage CEWs and body cameras starting with the physical device. Toggle: Exempt this application from IP restrictions (disabled).
- Axon Air:** Application used to pilot, livestream and upload evidence from unmanned aircraft systems. Toggle: Exempt this application from IP restrictions (disabled).
- Axon Aware:** Allows users to receive real-time alerts and view officer locations and live streams from a mobile device. Toggle: Exempt this application from IP restrictions (disabled).

3. Select the Axon Applications (Axon View, Axon Capture, Axon Device Manager, Axon Air, and Axon Aware) you want to exempt from IP Restrictions.

Return to the main System Administration page.

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 **Multi-Factor Authentication Settings (MFA)**.
2. 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.

3. 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.

4. 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.
5. 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.

- **Session Timeout** – Sets the number of minutes a user can be inactive before the user is automatically signed out of Evidence.com. [default 10, min 10, max 720]
- **Failed Login Limit** — Sets the number of failed login attempts before the account is locked out. [default 5, min 1, max 25]
- **Lockout Duration** — Sets the number of minutes a user is locked out of their account due to failed login attempts. [default 60, min 1, max 720]
- **Password History** — Sets the number of unique new passwords a user must use before an old password can be reused. [default 10, min 1, max 25]

- **Maximum Password Age** — Determines how many days a password can be used before the user is required to change it. [default 90, min 7, max 365]
- **Minimum Password Age** – Sets the number of days a user must wait between manually changing their password. This setting does not affect administrative password resets. [default 1, min 0, max 7]
- **Minimum Password Length** — Sets how short passwords can be. [default 8, min 6]
- **Password Character Requirements** – Sets the types of characters required in a user's password. Only the **Special Characters** option is editable. When enabled, users must include at least one special character in their password.

Note: There are no configuration settings for user security questions. Users have 15 attempts to enter their correct security question responses. User 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 **Reset to Defaults**.

3. When have finished configuring password settings, click **Save**.
4. On the notification message box, click **OK**.

API Settings

The API Settings section is only available to Axon Evidence agencies who request access to the Evidence.com Partner API. The Axon Evidence Partner API provides a programmatic means to access the data in your Axon Evidence agency. By developing API-compliant client software or using third-party client software, you can use the Partner API to integrate your Axon Evidence agency with other systems.

The API Settings page provides administrators with the ability to ensure that only authenticated and authorized clients can use the Partner API feature to programmatically configure your Axon Evidence agency. An API client can request, create, read, update and delete operations on a variety of data resources supported by the API, which include the following object types:

- Users
- Groups
- Cases
- Evidence
- Devices
- Reports
- Category Management

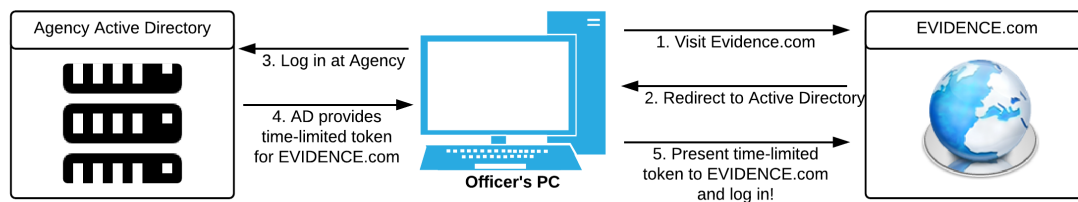
The Partner API is available to all Axon Evidence agencies. To request access to the Partner API, contact your Axon representative. If you need assistance developing API client software, Axon Professional Services are available for billable work.

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

Clicking this link takes you to the [Axon Evidence section of myAxon](#), which has information about the various features of Axon Evidence and other Axon products.

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. Some release notes also have a link to a video overview of the notes.

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.

Pre-Configured Role	Locked or Configurable	Required License Tier
Admin	Locked	Pro
User	Configurable	Basic (Pro if a Pro license permission is allowed)
Investigator	Configurable	Pro
Armorer	Configurable	Basic (Pro if a Pro license permission is allowed)
Lite User	Locked	N/A
Lite Armorer	Locked	N/A

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.

Permission	Requires Pro License?	Unlocked By:	Description
Login Access			
Evidence.com	No	—	Allows a user to log in to their agency's Evidence.com agency.
Evidence Sync	No	—	Allows a user to log in to Evidence Sync in Online mode. This permission also allows access to Axon Interview, if installed at the agency.
Axon Capture	No	—	Allows a user to log in to and upload files from the Axon Capture mobile application.
Axon View XL and Axon Fleet Dashboard	No	—	Allows a user to log in to Axon View XL and Axon Fleet Dashboard applications.
Axon Performance	No	—	Allows a user to log in to Axon Performance. Only visible if Axon Performance is enabled for your agency.
User Access			
Edit Account Information	No	—	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.
View Message Center	No	User Search	Allows a user to read messages sent from Evidence.com.
Download Sync Software	No	—	Allows a user to download Sync software from their Evidence.com agency.
Create/Edit Group	No	User Search	Allows a user to create a group and edit its monitors and members.
Group Audit Trail PDF	No	—	Allows a user to view an audit trail of the activities related to a group.
Admin Access			
Configure Agency Security Settings	No	—	Allows a user to edit the agency's IP Restrictions, authentication method, password configurations, partner agencies, and transcription accounts. For agencies with Single Sign-On (SSO) enabled, a user can bypass SSO to sign in with their Evidence.com credentials for troubleshooting. This permission is also used for the Axon Device Manager SSO bypass for third-party apps.
Edit Agency Settings	No	—	Allows a user to configure agency-wide settings including Field Validation, Retention Categories, Video and Camera Settings, CEW Setting, Roles and Permissions, and Password Configuration requirements.

Permission	Requires Pro License?	Unlocked By:	Description
Edit Device Offline & Microphone Settings	No	Edit Agency Settings	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.
CEW Administration (manage and reassign CEWs)	No	User Search, Inventory Search	Allows a user to search for reassign agency CEW and TASER CAM devices.
CEW Logs Administration (manage CEW logs)	No	User Search, Inventory Search, View CEW Firing Logs	Allows a user to view CEW logs, extract evidence from CEW logs, reassign log events and share logs with Axon.
Device Administration (manage non-CEW devices, reassign devices)	No	User Search and Inventory Search	Allows a user to reassign all agency non-CEW devices and change their settings.
Edit Agency Device Settings	No	User Search and Inventory Search	Allows a user to edit agency wide settings for all non-CEW devices.
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.
Category Administration	No	—	Allows a user to add a Category to the agency's list or edit an existing Category. It also allows a user to use the Extend option for extending the retention date for evidence.
Return Administration	No	User Search and Inventory Search	Allows a user to initiate, manage, and track device returns within Evidence.com.
Custom Metadata	No	—	Allows a user to create and update the configuration for custom metadata fields.
Search & Reporting Access			
User Search	No	—	Allows a user to see what users are in the agency. If disabled the user will be 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.

Permission	Requires Pro License?	Unlocked By:	Description
List Unrestricted Evidence	No	User Search	Allows a user to search for unrestricted evidence in the agency. Can be set to allow access to any evidence or only the user's evidence. Note: The user can only access the Evidence specified under the Evidence Management permissions.
List Restricted Evidence	No	User Search	Allows a user to search for restricted evidence in the agency. Can be set to allow access to any evidence or only the user's evidence. Note: The user can only access the Evidence specified under the Evidence Management permissions.
List Confidential Evidence	No	User Search	Allows a user to search for confidential evidence in the agency. Can be set to allow access to any evidence or only the user's evidence. Note: The user can only access the Evidence specified under the Evidence Management permissions.
Inventory Search	No	User Search	Allows a user to search for all of the Devices in the agency.
List Unrestricted Cases	No	User Search and Evidence Search	Allows a user to search for unrestricted Cases in an agency. Can be set to allow access to any case or only the user's cases. Note: Their ability to access a Case is determined by the Case Management Permissions.
List Restricted Cases	Yes	User Search and Evidence Search	Allows a user to search for restricted cases in the agency. Can be set to allow access to any case or only the user's cases. Note: Their ability to access a Case is determined by the Case Management Permissions.
List Confidential Cases	Yes	User Search and Evidence Search	Allows a user to search for confidential cases in the agency. Can be set to allow access to any case or only the user's cases. Note: Their ability to access a Case is determined by the Case Management Permissions.
Generate Reports	Yes	—	Allows a user to generate reports.
Generate User Audit Trail Report	Yes	Generate Reports	Allows a user to generate User Audit Trails from the Reports page.

Permission	Requires Pro License?	Unlocked By:	Description
Command Hierarchy			
Manage Command Hierarchy	No	Create/Edit Group	Allows a user to add, edit, or remove groups from the Command Hierarchy. This includes importing groups using a CSV file.
Evidence Creation			
Upload External Files	No	—	Allows a user to upload files through Evidence Sync, the Import Evidence feature, and Evidence Upload XT. 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.
Evidence Management			
View Unrestricted Evidence	No	List Unrestricted Evidence	Allows a user to access unrestricted evidence, except for weapon firing logs. Can be set to allow access to any evidence, their group's evidence, or only the user's evidence.
View Restricted Evidence	Yes	List Restricted Evidence	Allows a user to access restricted evidence, except for weapon firing logs. Can be set to allow access to any evidence, their group's evidence, or only the user's evidence.
View Confidential Evidence	Yes	List Confidential Evidence	Allows a user to access confidential evidence, except for weapon firing logs. Can be set to allow access to any evidence, their group's evidence, or only the user's evidence.
View CEW Firing Logs	No	List Unrestricted Evidence	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.
Edit	No	Evidence Management View Evidence	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.
Add/Remove Pending Review Category	No	Evidence Management Edit	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.

Permission	Requires Pro License?	Unlocked By:	Description
Edit Evidence Group	No	Evidence Management Edit	Allows a user to modify the evidence group for a piece of evidence.
Redact	Yes	Evidence Management Edit	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.
Order Human Transcript	Yes	Evidence Management View Evidence	Allows a user to order transcripts.
Auto-Transcribe	Yes	Evidence Management View Evidence	Allows the user to request an auto-transcript. This can be set to allow the user to request an auto-transcript for any evidence or only evidence belonging to the user or the user's groups.
Edit Auto-Transcript	Yes	Evidence Management View Evidence	Allows the user to access and use the Transcription Assistant to edit an auto-transcript. This can be set to allow the user to edit the auto-transcript for any evidence or only evidence belonging to the user or the user's groups.
Verify & Unverify Transcript	Yes	Evidence Management View Evidence and Evidence Management Edit Auto-Transcript	Allows the user to verify and unverify an auto-transcript. This can be set to allow the user to verify and unverify the auto-transcript for any evidence or only evidence belonging to the user or the user's groups.
Reassign	No	User Search and Evidence Management View Evidence	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.
Delete Evidence & Edit Date Recorded	No	Evidence Management View Evidence	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.
Download	No	Evidence Management View Evidence	Allows a user to download Evidence. Can be set to allow access to any evidence or only the user's evidence.
Download Infected Files	No	Evidence Management Download	Allows a user to download Evidence that either failed a malware scan or is currently being scanned.
Share	No	User Search and Evidence Management View Evidence	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.

Permission	Requires Pro License?	Unlocked By:	Description
Publish to Social Media	No	Evidence Management View Evidence	Allows a user to publish content directly to approved social media platforms.
Apply Access Class – Restricted	No	Evidence Management View and Evidence Management Share	<p>Allows users to apply the Restricted access class to evidence. Can be set to allow this action for any evidence, the user's group, or only the user's evidence.</p> <p>Note: If a user does not have permission to apply the Restricted or Confidential access class, then the user will not be able to assign evidence to a category that applies the access class change in Axon Evidence. Users applying categories using Axon mobile or desktop apps are not restricted from assigning categories.</p>
Remove Access Class – Restricted	No	Evidence Management View Evidence	Allows users to remove the Restricted access class from evidence. Can be set to allow this action for any evidence, the user's group, or only the user's evidence.
Apply Access Class – Confidential	Yes	Evidence Management View Evidence and Evidence Management Share	<p>Allows users to apply the Confidential access class to evidence. Can be set to allow this action for any evidence, the user's group, or only the user's evidence.</p> <p>Note: If a user does not have permission to apply the Restricted or Confidential access class, then the user will not be able to assign evidence to a category that applies the access class change in Axon Evidence. Users applying categories using Axon mobile or desktop apps are not restricted from assigning categories.</p>
Remove Access Class – Confidential	Yes	Evidence Management View	Allows users to remove the Confidential access class from evidence. Can be set to allow this action for any evidence, the user's group, or only the user's evidence.
Share Externally to Authenticated Users	No	Partner Contact Search, Evidence and Management Share	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.

Permission	Requires Pro License?	Unlocked By:	Description
Share External Download Links	No	Evidence Management Share and Evidence Management Download	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.
Add & Edit Notes	No	Evidence Management View Evidence	Allows a user to add messages to Evidence, edit messages, and delete their own messages. Can be set to allow access to any evidence or only the user's evidence.
Audit Trail PDF	No	Evidence Management View	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.
Access Video Recall Files	No	Evidence Management View Evidence	Allows a user to view a list of Video Recall files on a camera and choose which ones to upload.
Access evidence in their Command	No	Appropriate Evidence Management permissions set to Their group and their own.	Allows a user to perform an action (view, edit, etc.) on evidence where the Evidence Group is set to their Command Hierarchy Group or a subordinate (child) group. Note: This permission requires that the role has the appropriate Evidence Management permissions (View Unrestricted Evidence, View Restricted Evidence, View Confidential Evidence, Apply and Remove Access Class, Edit and Edit Evidence Group) set to Their group and their own.
Access evidence uploaded by Users in the Command	No	Appropriate Evidence Management permissions set to Their group and their own.	Allows a user to perform an action (view, edit, etc.) on evidence that was uploaded by users in their Command Hierarchy Group and subordinate (child) groups. Note: This permission requires that the role has the appropriate Evidence Management permissions (View Unrestricted Evidence, View Restricted Evidence, View Confidential Evidence, Apply and Remove Access Class, Edit and Edit Evidence Group) set to Their group and their own.

Permission	Requires Pro License?	Unlocked By:	Description
Case Management			
View Unrestricted Cases	No	List Unrestricted Cases	Allows a user to access an unrestricted Case. Can be set to allow access to any case or only the user's cases.
View Restricted Cases	No	List Restricted Cases	Allows a user to access a restricted Case. Can be set to allow access to any case or only the user's cases.
View Confidential Cases	No	List Confidential Cases	Allows a user to access a confidential Case. Can be set to allow access to any case or only the user's cases.
Edit	No	Case Management View Cases	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.
Reassign	No	User Search, Case Management View Cases and Case Management Edit,	Allows a user to change the Owner of a Case. Can be set to allow access to any case or only the user's cases.
Share	No	User Search and Case Management View, Evidence Management Share	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.
Apply Access Class – Restricted	No	Evidence Management Apply Access Class - Restricted, Case Management View, and Case Management Share	Allows users to apply the Restricted access class to a case. Can be set to allow access to any case or only the user's cases
Remove Access Class – Restricted	No	Evidence Management Remove Access Class - Restricted, Case Management View	Allows users to remove the Restricted access class from a case. Can be set to allow access to any case or only the user's cases

Permission	Requires Pro License?	Unlocked By:	Description
Apply Access Class – Confidential	No	Evidence Management Restrict, Case Management View, Case Management Share	Allows users to apply the Confidential access class to a case. Can be set to allow access to any case or only the user's cases
Remove Access Class – Confidential	No	Evidence Management Restrict, Case Management View, Case Management Share	Allows users to remove the Confidential access class from a case. Can be set to allow access to any case or only the user's cases
Share with Partner Agencies	No	Partner Contact Search, Case Management Share, and Evidence Management Share Externally to Authenticated Users	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.
Share External Download Links	No	Case Management Share and Evidence Management Share External Download Links	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.
Audit Trail PDF	No	Case Management View Cases	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.
Add & Edit Notes	No	Case Management Edit	Allows a user to add messages to a Case, edit messages, and delete their own messages. Can be set to allow access to any case or only the user's cases.
Edit Case Retention	No	Case Management Edit	Allows a user to update the retention policy for cases. Can be set to allow access to any case or only the user's cases.

Permission	Requires Pro License?	Unlocked By:	Description
Create Case	No	Evidence Management Search, Case Management Search, Case Management Edit	Allows a user to create a Case.
Citizen Management			
View Portals (Individual and Public)	No	—	Allows a user to view information about a portal, but not edit the information or view triage submissions.
Invite Individual	No	Citizen Management View Portals	Allows a user to create an individual portal for an individual citizen.
Create Public Portal	No	—	Allows a user to create a public portal that can be used by the community to upload items.
Edit and Close Public Portal	No	Citizen Management View Portals	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.
Triage Submissions	No	Evidence Management View Citizen Management View Portals	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.
Audit Trail PDF	No	Citizen Management View Portals	Allows a user to view and download a PDF record of who has viewed, edited or triaged portals.
Axon Performance (Only visible if Axon Performance is enabled for the agency)			
Configure Performance Settings	No	—	Allows users to configure Axon Performance in accordance with agency policies.
View Squad Performance	No	—	Allows users to view squad performance information. This can be set to allow the user to view information for any squad or only those where the user is assigned as the supervisor.
View Video Review	No	View Squad Performance	Allows users to view the results of random video reviews. This can be set to allow the user to view information for any officer or only those where the user is assigned as the supervisor. To allow the user to view information for any squad, the View Squad Performance permission must be set to Any.

Permission	Requires Pro License?	Unlocked By:	Description
Initiate Video Review	No	View Video Review	Allows users to conduct random video reviews. This can be set to allow the user to review any officer video or only those where the user is assigned as the supervisor. To allow the user to review any officer video, the View Video Review permission must be set to Any.
View Policy Review	No	View Squad Performance	Allows users to view officer policy reviews. This can be set to allow the user to view information for any officer or only those where the user is assigned as the supervisor. To allow the user to view information for any squad, the View Squad Performance permission must be set to Any.
Initiate Policy Review	No	View Policy Review	Allows users to conduct officer policy reviews. This can be set to allow the user to review any officer or only those where the user is assigned as the supervisor. To allow the user to view information for any officer, the View Policy Review permission must be set to Any.
Axon Respond (Only visible if Axon Respond for Devices is enabled for the agency)			
View Location Map	No	—	Allows the user to access the Respond map and view camera locations.
Live Stream	No	View Location Map	Allows the user to view camera livestreams for the Respond map.
View Respond Audit Log	No	—	Allows a user to view and download the record of all Axon Respond for Devices activity.
Mark Alert as False or Resolved	No	View Location Map	Allows the user to mark an alert (gunshot or CEW) as false or resolved in Axon Respond.
Email Notification Preferences			
Account Lockout Notification	No	User Administration	Determines whether or not a user can receive Account Lockout Notifications when any user in the agency is locked out, External Agency Collaboration Notifications for collaborating with and sharing evidence to other agencies, and Category Assignment Notifications when evidence is assigned to at least one category that is being deleted. These emails can be disabled by the user from the user's User Profile – Notifications page.
Upcoming Evidence Deletion Notification	No	User Administration	Determines whether or not a user can receive weekly notifications of any upcoming evidence deletions in the agency. This email can be disabled by the user from the user's User Profile – Notifications page.

Permission	Requires Pro License?	Unlocked By:	Description
Evidence Timestamp Notification	No	User Administration or Edit Account Information	Determines whether or not a user can receive weekly notifications of evidence whose timestamp indicates it is older than 14 days. This email can be disabled by the user from the user's User Profile – Notifications page.
Axon Evidence and Performance Service Impact Notification	No	User Administration	Determines whether or not a user will receive email notifications of service outages or degradation for Axon Evidence and Axon Performance.
Axon Respond for Devices Service Impact Notification	No	User Administration	Determines whether or not a user will receive email notifications of service outages or degradation for Axon Respond for Devices.
Axon Respond for Dispatch Service Impact Notification	No	User Administration	Determines whether or not a user will receive email notifications of service outages or degradation for Axon Respond for Dispatch.
Axon Records and Standards Service Impact Notification	No	User Administration	Determines whether or not a user will receive email notifications of service outages or degradation for Axon Records and Standards.
Axon Product Release Notes Notification	No	User Administration	Determines whether or not a user will receive release note emails for Axon Evidence, Axon Body-Worn Cameras, Axon Fleet, and other Axon products.
System Status			
View Status Page	No	—	Allows a user to view the Axon System Status Page.
ALPR			
Read/Hit Record Search	No	—	Allows a user to search and view any agency ALPR.
Hotlist Management	No	—	Allows a user to search, modify, and create agency hotlists.
ALPR System Administration	No	—	Allows a user to modify agency-level ALPR settings, such as record retention and alert categories.

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.

Permission	Admin	User	Investigator	Armorer
Login Access				
Evidence.com	Allowed	Allowed	Allowed	Allowed
Evidence Sync	Allowed	Allowed	Allowed	Allowed
Axon Capture	Allowed	Allowed	Allowed	Prohibited
Axon View XL and Axon Fleet Dashboard	Allowed		Allowed	Prohibited
Axon Performance	Allowed	Prohibited	Prohibited	Prohibited
User Access				
Edit Account Information	Allowed	Allowed	Allowed	Allowed
View Message Center	Allowed	Allowed	Allowed	Prohibited
Download Sync Software	Allowed	Allowed	Allowed	Allowed
Create/Edit Group	Allowed	Prohibited	Prohibited	Prohibited
Group Audit Trail PDF	Allowed	Prohibited	Prohibited	Prohibited
Admin Access				
Configure Agency Security Settings	Allowed	Prohibited	Prohibited	Prohibited
Edit Agency Settings	Allowed	Prohibited	Prohibited	Prohibited
Edit Device Offline & Microphone Settings	Allowed	Prohibited	Prohibited	Prohibited
CEW Administration	Allowed	Prohibited	Prohibited	Allowed
CEW Logs Administration	Allowed	Prohibited	Prohibited	Allowed
Device Administration	Allowed	Prohibited	Prohibited	Allowed
Edit Agency Device Settings	Allowed	Prohibited	Prohibited	Prohibited
User Administration	Allowed	Prohibited	Allowed	Prohibited
Category Administration	Allowed	Prohibited	Allowed	Prohibited
Return Administration	Allowed	Prohibited	Prohibited	Allowed
Custom Metadata	Allowed	Prohibited	Prohibited	Prohibited
Search & Reporting Access				
User Search	Allowed	Allowed	Allowed	Allowed
Partner Contact Search	Allowed	Allowed	Prohibited	Prohibited

Permission	Admin	User	Investigator	Armorer
List Unrestricted Evidence	Any Evidence	Any Evidence	Any Evidence	Any Evidence
List Restricted Evidence	Any Evidence	Any Evidence	Any Evidence	Any Evidence
List Confidential Evidence	Prohibited	Prohibited	Prohibited	Prohibited
Inventory Search	Allowed	Allowed	Allowed	Allowed
List Unrestricted Cases	Any Case	Any Case	Any Case	Any Case
List Restricted Cases	Any Case	Any Case	Any Case	Any Case
List Confidential Cases	Prohibited	Prohibited	Prohibited	Prohibited
Generate Reports	Allowed	Prohibited	Allowed	Prohibited
Generate User Audit Trail Report	Allowed	Prohibited	Prohibited	Prohibited
Command Hierarchy				
Manage Command Hierarchy	Allowed	Prohibited	Prohibited	Prohibited
Evidence Creation				
Upload External Files	Allowed	Allowed	Allowed	Prohibited
Configure Automatic Upload through Evidence Sync	Allowed	Prohibited	Prohibited	Prohibited
Evidence Management				
View Unrestricted Evidence	Any Evidence	Only Their Own	Only Their Own	Only Their Own
View Restricted Evidence	Prohibited	Prohibited	Prohibited	Prohibited
View Confidential Evidence	Prohibited	Prohibited	Prohibited	Prohibited
View CEW Firing Logs	Any Evidence	Only Their Own	Only Their Own	Only Their Own
Edit	Any Evidence	Only Their Own	Only Their Own	Prohibited
Add/Remove Pending Review Category	Any Evidence	Only Their Own	Prohibited	Prohibited
Edit Evidence Group	Any Evidence	Prohibited	Prohibited	Prohibited
Redact	Any Evidence	Only Their Own	Only Their Own	Prohibited
Order Human Transcript	Allowed	Prohibited	Prohibited	Prohibited
Auto-Transcribe	Any Evidence	Prohibited	Prohibited	Prohibited
Edit Auto-Transcript	Any Evidence	Prohibited	Prohibited	Prohibited
Verify & Unverify Transcript	Any Evidence	Prohibited	Prohibited	Prohibited
Reassign	Any Evidence	Only Their Own	Only Their Own	Prohibited
Delete Evidence & Edit Date Recorded	Any Evidence	Prohibited	Prohibited	Prohibited

Permission	Admin	User	Investigator	Armorer
Download	Any Evidence	Only Their Own	Only Their Own	Prohibited
Download Infected Files	Allowed	Prohibited	Prohibited	Prohibited
Share	Any Evidence	Only Their Own	Only Their Own	Prohibited
Publish to Social Media	Allowed	Prohibited	Prohibited	Prohibited
Apply Access Class – Restrict	Any Evidence	Prohibited	Prohibited	Prohibited
Remove Access Class – Restrict	Any Evidence	Prohibited	Prohibited	Prohibited
Apply Access Class – Confidential	Prohibited	Prohibited	Prohibited	Prohibited
Remove Access Class – Confidential	Prohibited	Prohibited	Prohibited	Prohibited
Share Externally to Authenticated Users	Allowed	Allowed	Prohibited	Prohibited
Share External Download Links	Allowed	Prohibited	Prohibited	Prohibited
Add & Edit Notes	Any Evidence	Only Their Own	Only Their Own	Prohibited
Audit Trail PDF	Any Evidence	Only Their Own	Only Their Own	Prohibited
Access Video Recall Files	Allowed	Prohibited	Prohibited	Prohibited
Access evidence in their Command	Allowed	Prohibited	Prohibited	Prohibited
Access evidence uploaded by Users in their Command	Allowed	Prohibited	Prohibited	Prohibited
Case Management				
View Unrestricted Cases	Any Case	Only Their Own	Any Case	Only Their Own
View Restricted Cases	Prohibited	Prohibited	Prohibited	Prohibited
View Confidential Cases	Prohibited	Prohibited	Prohibited	Prohibited
Edit	Any Case	Only Their Own	Any Case	Prohibited
Reassign	Any Case	Only Their Own	Any Case	Prohibited
Share	Any Case	Only Their Own	Only Their Own	Prohibited
Apply Access Class – Restrict	Any Case	Prohibited	Prohibited	Prohibited
Remove Access Class – Restrict	Any Case	Prohibited	Prohibited	Prohibited
Apply Access Class – Confidential	Prohibited	Prohibited	Prohibited	Prohibited
Remove Access Class – Confidential	Prohibited	Prohibited	Prohibited	Prohibited
Share with Partner Agencies	Allowed	Prohibited	Prohibited	Prohibited
Share External Download Links	Allowed	Prohibited	Prohibited	Prohibited
Audit Trail PDF	Any Case	Only Their Own	Any Case	Prohibited

Permission	Admin	User	Investigator	Armorer
Add & Edit Notes	Any Case	Only Their Own	Any Case	Prohibited
Edit Case Retention	Any Case	Prohibited	Prohibited	Prohibited
Create Case	Allowed	Allowed	Allowed	Prohibited
Citizen Management				
View Portals (Individual and Public)	Any Portal	Prohibited	Prohibited	Prohibited
Invite Individual	Allowed	Prohibited	Prohibited	Prohibited
Create Public Portal	Allowed	Prohibited	Prohibited	Prohibited
Edit and Close Public Portal	Any Portal	Prohibited	Prohibited	Prohibited
Triage Submissions	Any Portal	Prohibited	Prohibited	Prohibited
Audit Trail PDF	Any Portal	Prohibited	Prohibited	Prohibited
Axon Performance				
Configure Performance Settings	Allowed	Prohibited	Prohibited	Prohibited
View Squad Performance	Any	Prohibited	Prohibited	Prohibited
View Video Review	Any	Prohibited	Prohibited	Prohibited
Initiate Video Review	Any	Prohibited	Prohibited	Prohibited
View Policy Review	Any	Prohibited	Prohibited	Prohibited
Initiate Policy Review	Any	Prohibited	Prohibited	Prohibited
Axon Respond				
View Location Map	Allowed	Prohibited	Prohibited	Prohibited
Live Stream	Allowed	Prohibited	Prohibited	Prohibited
View Respond Audit Log	Allowed	Prohibited	Prohibited	Prohibited
Mark Alert as False or Resolved	Allowed	Prohibited	Prohibited	Prohibited
Email Notification Preferences				
Account Lockout Notification	Allowed	Prohibited	Allowed	Prohibited
Upcoming Evidence Deletion Notification	Allowed	Prohibited	Allowed	Prohibited
Evidence Timestamp Notification	Allowed	Prohibited	Allowed	Prohibited
Axon Evidence and Performance Service Impact Notification	Allowed	Prohibited	Prohibited	Prohibited
Axon Respond for Devices Service Impact Notification	Allowed	Prohibited	Prohibited	Prohibited
Axon Respond for Dispatch Service Impact Notification	Allowed	Prohibited	Prohibited	Prohibited
Axon Records and Standards Service Impact Notification	Allowed	Prohibited	Prohibited	Prohibited
Axon Product Release Notes Notification	Allowed	Prohibited	Prohibited	Prohibited
System Status				

Permission	Admin	User	Investigator	Armorer
View Status Page	Allowed	Prohibited	Prohibited	Prohibited
ALPR				
Read/Hit Record Search	Allowed	Prohibited	Prohibited	Prohibited
Hotlist Management	Allowed	Prohibited	Prohibited	Prohibited
ALPR System Administration	Allowed	Prohibited	Prohibited	Prohibited

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.

Permission	Lite User	Lite Armorer
Login Access		
Evidence.com	Allowed	Allowed
Evidence Sync	Allowed	Allowed
Axon Capture	Prohibited	Prohibited
Axon View XL and Axon Fleet Dashboard	Prohibited	Prohibited
Axon Performance	Prohibited	Prohibited
User Access		
Edit Account Information	Allowed	Allowed
View Message Center	Allowed	Allowed
Download Sync Software	Allowed	Allowed
Create/Edit Group	Prohibited	Prohibited
Group Audit Trail PDF	Prohibited	Prohibited
Admin Access		
Configure Agency Security Settings	Prohibited	Prohibited
Edit Agency Settings	Prohibited	Prohibited
Edit Device Offline & Microphone Settings	Prohibited	Prohibited
CEW Administration	Prohibited	Allowed
CEW Logs Administration	Prohibited	Allowed
Device Administration	Prohibited	Prohibited
Edit Device Agency Settings	Prohibited	Prohibited
User Administration	Prohibited	Prohibited
Category Administration	Prohibited	Prohibited
Return Administration	Prohibited	Allowed

Permission	Lite User	Lite Armorer
Custom Metadata	Prohibited	Prohibited
Search & Reporting Access		
User Search	Prohibited	Allowed
Partner Contact Search	Prohibited	Prohibited
List Unrestricted Evidence	Only Their Own	Prohibited
List Restricted Evidence	Prohibited	Prohibited
List Confidential Evidence	Prohibited	Prohibited
Inventory Search	Prohibited	Allowed
List Unrestricted Cases	Prohibited	Prohibited
List Restricted Cases	Prohibited	Prohibited
List Confidential Cases	Prohibited	Prohibited
Generate Reports	Prohibited	Prohibited
Generate User Audit Trail Report	Prohibited	Prohibited
Command Hierarchy		
Manage Command Hierarchy	Prohibited	Prohibited
Evidence Creation		
Upload External Files	Prohibited	Prohibited
Configure Automatic Upload through Evidence Sync	Prohibited	Prohibited
Evidence Management		
View Unrestricted Evidence	Prohibited	Prohibited
View Restricted Evidence	Prohibited	Prohibited
View Confidential Evidence	Prohibited	Prohibited
View CEW Firing Logs	Only Their Own	Only Their Own
Edit	Prohibited	Prohibited
Add/Remove Pending Review Category	Prohibited	Prohibited
Edit Evidence Group	Prohibited	Prohibited
Redact	Prohibited	Prohibited
Order Human Transcript	Prohibited	Prohibited
Auto-Transcribe	Prohibited	Prohibited
Edit Auto-Transcript	Prohibited	Prohibited
Verify & Unverify Transcript	Prohibited	Prohibited
Reassign	Prohibited	Prohibited
Delete Evidence & Edit Date Recorded	Prohibited	Prohibited
Download	Prohibited	Prohibited
Download Infected Files	Prohibited	Prohibited
Share	Prohibited	Prohibited

Permission	Lite User	Lite Armorer
Publish to Social Media	Prohibited	Prohibited
Apply Access Class – Restricted	Prohibited	Prohibited
Remove Access Class – Restricted	Prohibited	Prohibited
Apply Access Class – Confidential	Prohibited	Prohibited
Remove Access Class – Confidential	Prohibited	Prohibited
Share Externally to Authenticated Users	Prohibited	Prohibited
Share External Download Links	Prohibited	Prohibited
Add & Edit Notes	Prohibited	Prohibited
Audit Trail PDF	Prohibited	Prohibited
Access Video Recall Files	Prohibited	Prohibited
Access evidence in their Command	Prohibited	Prohibited
Access evidence uploaded by Users in their Command	Prohibited	Prohibited
Case Management		
View Unrestricted Cases	Prohibited	Prohibited
View Restricted Cases	Prohibited	Prohibited
View Confidential Cases	Prohibited	Prohibited
Edit	Prohibited	Prohibited
Reassign	Prohibited	Prohibited
Share	Prohibited	Prohibited
Apply Access Class – Restricted	Prohibited	Prohibited
Remove Access Class – Restricted	Prohibited	Prohibited
Apply Access Class – Confidential	Prohibited	Prohibited
Remove Access Class – Confidential	Prohibited	Prohibited
Share with Partner Agencies	Prohibited	Prohibited
Share External Download Links	Prohibited	Prohibited
Audit Trail PDF	Prohibited	Prohibited
Add & Edit Notes	Prohibited	Prohibited
Edit Case Retention	Prohibited	Prohibited
Create Case	Prohibited	Prohibited
Citizen Management		
View Portals (Individual and Public)	Prohibited	Prohibited
Invite Individual	Prohibited	Prohibited
Create Public Portal	Prohibited	Prohibited
Edit and Close Public Portal	Prohibited	Prohibited
Triage Submissions	Prohibited	Prohibited
Audit Trail PDF	Prohibited	Prohibited

Permission	Lite User	Lite Armorer
Axon Performance		
Configure Performance Settings	Prohibited	Prohibited
View Squad Performance	Prohibited	Prohibited
View Video Review	Prohibited	Prohibited
Initiate Video Review	Prohibited	Prohibited
View Policy Review	Prohibited	Prohibited
Initiate Policy Review	Prohibited	Prohibited
Axon Respond		
View Location Map	Prohibited	Prohibited
Live Stream	Prohibited	Prohibited
View Respond Audit Log	Prohibited	Prohibited
Mark Alerts as False or Resolved	Prohibited	Prohibited
Email Notification Preferences		
Account Lockout Notification	Prohibited	Allowed
Upcoming Evidence Deletion Notification	Prohibited	Prohibited
Evidence Timestamp Notification	Prohibited	Prohibited
Axon Evidence and Performance Service Impact Notification	Prohibited	Prohibited
Axon Respond for Devices Service Impact Notification	Prohibited	Prohibited
Axon Respond for Dispatch Service Impact Notification	Prohibited	Prohibited
Axon Records and Standards Service Impact Notification	Prohibited	Prohibited
Axon Product Release Notes Notification	Prohibited	Prohibited
System Status		
View Status Page	Prohibited	Prohibited
ALPR		
Read/Hit Record Search	Prohibited	Prohibited
Hotlist Management	Prohibited	Prohibited
ALPR System Administration	Prohibited	Prohibited

Appendix B: Traditional Media Player

The procedures for working with the traditional media player were removed from the guide PDF to reduce the size of the guide. If you need a copy of the procedures, contact Technical Support and request a copy of the Traditional Media Player procedures.

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 3 Camera Settings Descriptions

Video

- **Quality (Default – 720p High)**

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 720p High.

- **Pre-event buffer (Default – 30 seconds)**

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.

- **Watermark (Default – Enabled)**

This sets if a permanent watermark appears in the upper right corner of 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.

- **Watermark local time zone (Default – Enabled)**

This determines the time zone displayed in the permanent watermark. When enabled, the local time zone, based on agency configuration, is used. When disabled, UTC is used.

- **Video Recall** (Note: This setting is disabled by default and changing the setting will have no effect on your agency's Axon Body 3 cameras until camera OS v1.13 is available.)

This setting enables the upcoming Video Recall feature, which would be applied to all agency devices. This feature allows authorized users to upload and review video captured by an Axon Body 3 camera when the camera is on but not actively recording. The recalled evidence will be of lower quality and without audio. It is saved to the camera buffer, which, with Video Recall enabled, is overwritten after 18 hours. More information about the Video Recall feature will be available in future updates.

Audio

- **Audio recording (Default – Enabled)**

This sets if the camera records audio while recording video.

Note that if the **Users can mute during recording** setting is enabled, users will have the ability to turn audio recording for their camera on and off.

- **Pre-event buffer (Default – Disabled)**

This sets if audio is recorded in the pre-event buffer.

- **Audio in Video Recall (Default – Disabled)**

Enables audio recording while cameras are capturing video recall evidence. The setting is only visible if the **Video Recall** setting is enabled.

Lights

- **Front light (Default – Disabled)**

This setting enables the visible indication of the recording status on the front triad LEDs. During pre-event buffering, the LEDs blink green. During recording the LEDs blink red. Stealth Mode must be disabled for this setting to be enabled.

- **Automatic Brightness (Default – Disabled)**

Note: This feature requires Axon Body 3 OS v1.11 or higher.

Enables LED Auto Brightness mode for Axon Body 3 cameras. This mode automatically adjusts the brightness of front and top LED lights based on ambient light. If front lights are disabled, the changes only apply to top light. Users must have permission to adjust indicator lights to enable Auto mode from the camera or Axon

applications. Additionally, Stealth mode must be disabled for this setting to be enabled.

Location

- **Record location in video (Default – Enabled)**

This setting determines if GPS data is embedded when videos are being recorded

- **Make location information available to Axon Respond (Default – Location available when camera is recording)**

Only available if Axon Respond for Devices is enabled for your agency.

This setting determines if location information is made available in near real-time to authorized agency users.

When the **Location available when camera is recording and buffering** setting is selected, camera location will be reported to Axon Respond and Axon Evidence while the camera is recording and while the camera is buffering. Location will be available in both the browser and mobile application of Axon Respond. Camera location while the camera is buffering is updated on the Respond platforms every 15 minutes and will be denoted on the map as device markers. Camera location while recording is updated every few seconds. The location map on the Axon Evidence Device Profile page is updated with the same frequency as the Respond platform.

Important: Choosing the **Location available when camera is recording and buffering** setting will have an impact on battery charge levels. Users can expect to see a 5 to 10 minute reduction in total camera runtime when the option is selected.

- **Wi-Fi Positioning (Default – Enabled)**

This setting determines if Wi-Fi access points are used to determine location based on Wi-Fi signal strength. Enabling Wi-Fi positioning allows the camera's Wi-Fi capabilities to be used to assist in determining location, which improves overall location accuracy, allowing for indoor location determination, as well as reduced time to "first fix" for the camera's GPS.

Signal

- **Signal (Default – Disabled)**

This setting determines the camera's ability to activate recording by Axon Signal products. If disabled, cameras will not activate when notified by Axon Signal products.

The trigger events for the cameras are set on the Signal Configuration page.

- **False Signal Cancellation (Default – Disabled)**

Determines if Signal alerts can be canceled on the camera. Users can dismiss a Signal alert by pressing the Select button.

- **False gunshot cancellation default category (Default – Uncategorized)**

Only active if **False Signal Cancellation** is enabled.

Select the category automatically applied to recordings cancelled as false activations.

Streaming

- **Live streaming (Default – Enabled)**

Only available if Axon Respond for Devices with a Device + license is enabled for your agency.

This setting determines if cameras can stream audio and video while recording to authorized agency users.

Gunshot Detection

- **Gunshot detection recording (Default – Disabled)**

This setting determines if the camera starts recording if sensors detect the camera wearer discharged a firearm.

- **Gunshot detection notification (Default – Disabled)**

Only available if Axon Respond for Devices is enabled for your agency.

This setting determines if a notification is made available in near real-time to authorized agency users.

- **False gunshot detection cancellation (Default – Disabled)**

Determines if gunshot alerts can be canceled on the camera. Users can dismiss a false gunshot detection by pressing the Select button.

- **False gunshot cancellation default category (Default – Uncategorized)**

Only active if the False gunshot detection cancellation is enabled.

Select the category automatically applied to recordings cancelled as false activations.

App Support

- **Axon View pairing (Default – Enabled)**

This setting determines if cameras can pair with Axon View.

- **Video playback from device (Default – Enabled)**

This setting determines if users can playback video while it is still on the camera from Axon View or Axon View XL.

- **Axon View XL Upload**

This setting determines if users can upload videos on and Axon Body 3 camera using Axon View XL. This setting applies to both priority uploads from Axon Body 3 cameras paired with Axon View XL as part of an Axon Fleet installation and cameras connected to Axon View XL Standalone mode.

Evidence Upload

- **Automatic Wi-Fi Upload**

This setting determines if cameras can upload video through a connection with nearby agency trusted Wi-Fi Access Points. Agency trusted Wi-Fi Access Points are set on the [Body Camera Wi-Fi Networks page](#).

- **Priority Evidence Upload (Default – Disabled)**

Note: This feature requires Axon Body 3 OS v1.11 or higher.

This setting determines if users can select evidence for wireless upload from an Axon Body 3 camera. This option is only available for agencies with Axon Respond for Devices+ licenses. With the initial release, the camera user can choose to upload the most recently recorded piece of evidence on the device to Axon Evidence using the camera's LTE connectivity.

- **Apply rate-limiting to camera upload speed (Default – Disabled)**

This setting determines if a cameras' evidence upload speed is throttled when docked. If enabled, the maximum MB per second limit can be entered. This limit applies to each camera individually.

Firmware Download

- **Firmware download timeframe (Default – 6 hours)**

This setting allows agencies to adjust the timeframe in which cameras will download an operating system (OS) update in order to reduce network bandwidth strain. Agencies that experience network congestion during OS updates are advised to

extend the Firmware Download Timeframe setting to 8 hours, the maximum setting value. This means that the OS updates will be randomly received by all docked cameras over an 8 hour period, putting less strain on the network. The Firmware Download Timeframe can be set from 2 to 8 hours in 1 hour increments.

User Permissions

- **Users can mute during recording (Default – Enabled)**

This setting determines whether users can mute audio while recording an event. If allowed, users can mute audio recording using an on-camera button.

- **Users can adjust indicator light settings (Default – Enabled)**

This setting determines whether users can adjust the settings for the indicator lights of their camera. If allowed, users can turn on or off the indicator lights using an on-camera button, or with Axon View, Axon View XL, and Axon Evidence.

- **Users can adjust vibration settings (Default – Enabled)**

This setting determines whether users can adjust the vibration settings (haptic) of their camera. If allowed, users can turn on or off vibration settings with Axon View, Axon View XL, and Axon Evidence.

- **Users can use stealth mode (Default – Enabled)**

This setting determines whether users can go into stealth mode on their camera. If allowed, users can enter and exit stealth mode using an on-camera button, or with Axon View, Axon View XL, and Axon Evidence.

- **Users can use sleep mode (Default – Disabled)**

This setting determines whether users can go into sleep mode on their camera. Sleep mode puts the camera in an idle state that disables recording and buffering. This can be used as an alternative to powering off the camera. Sleep Mode provides a less than 4 second transition into this idle state and back into buffering or recording.

- **Settings return to default in dock** (Note This setting is disabled by default and changing the setting will have no effect on your agency's Axon Body 3 cameras until camera OS v1.13 is available.)

This setting determines whether camera settings that users can change will return to default agency settings when camera is docked.

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 with a setting for 10 seconds and 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 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.

- **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 ViewXL Pairing**

This sets if the cameras can be paired with the Axon ViewXL mobile application for Axon Fleet and Axon Fleet 2.

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.

- **Offline Configuration**

This sets if Axon Body 2 and Axon Flex 2 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.

- **Enhanced Low Power Warnings**

This setting adjusts the in-field Battery LED colors and enables a robust audio warning system when the camera is low on battery. The in-field Battery LED status indicator is green above 66%, yellow between 66% and 33%, red below 33%, and blinking red and yellow when critically low. The audio warning consists of 4 audio beeps and haptic vibrations at 20%, 15%, 10%, and 5% battery. Immediately before the device shuts down due to low power, it will emit an extra-long audio beep and haptic vibration.

The setting is disabled by default, but Axon recommends that you enable the setting for your Axon Body 2 and Axon Flex 2 cameras. When the setting is enabled, the warnings will be turned on the next time the camera or controller is placed in an Axon Dock.

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.

Additional Settings

- **Offline Configuration**

This sets if Axon Body 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 3 Settings

This appendix provides additional details for each of the Axon Fleet 3 camera settings. The quality settings can be set separately for the Fleet Dual-View and Interior Cameras. When Dashboard is connected to Axon Evidence, it automatically checks for and applies any updated Axon Fleet 3 configuration settings every 10 minutes.

Video Settings

- **Video Quality**

This setting controls the video quality for Fleet camera recordings. Higher quality videos will take up more storage space. Each Fleet camera can have a different setting.

For the best balance of quality and storage space, Axon recommends that the cameras record in HD 16:9 or HD 4:3.

- **Pre-Event Buffering**

This setting determines if video will be recorded in the pre-event buffer.

- **Watermark**

This setting determines whether 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.

To document video attribution during playback outside of Axon Evidence, Axon recommends enabling the Watermark feature.

Why does the Watermark default to 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.

After uploading, Axon Evidence converts the time for each video to local time shown in the upper right corner next to the video player.

- **Watermark in Local Time**

Sets the time zone displayed in the permanent watermark to the local time zone based on agency configuration.

- **Video Recall**

Enables powered Fleet 3 cameras to constantly capture video when not actively recording. Video recall stores a maximum of 24 hours of video per camera, continually overwriting the oldest video segments to make room for new. Video recall quality is preconfigured to 480p at 30fps with no audio. Recall is not overwritten by event recording. Other settings note if they affect recall. The ability for a user to recall videos is controlled by a Role permission.

Axon recommends enabling Video Recall.

Audio Settings

- **Audio Recording**

This setting determines if the Fleet 3 cameras record audio while recording video. Audio can include valuable information not conveyed in video.

Axon recommends enabling audio recording.

- **Pre-event Buffer Audio Recording**

This setting determines if audio is recorded in the pre-event buffer. Audio can include valuable information not conveyed in video.

Axon recommends enabling audio recording in the Per-event Buffer.

Lights Settings

- **Dual-View Camera LED Behavior**

Sets the behavior of the camera-side LED for Dual-View Cameras (typically facing out the front of the vehicle). During pre-event buffering the light will be solid green. During recording the light will blink red. Stealth Mode must be disabled for this setting to be enabled. These LEDs inform officers and the public when the system is recording,

Axon recommends enabling Dual-View Camera LEDs.

Location Settings

- **Record Location and Speed Information in Video**

This setting determines if GNSS/GPS location and speed data is saved in videos during recording.

Note: **Include Location Information in Axon Respond and Device Inventory**

This setting determines if GNSS/GPS location data is made available in near real-time to authorized agency users in Axon Respond and on the Axon Evidence Device page.

For the best Axon Respond experience, Axon recommends including location information for Axon Respond.

Respond Livestreaming Settings

- **Livestream**

This setting determines if the Dual-View camera can stream audio and video to authorized agency users while recording or while recording and buffering.

For the best balance of information and privacy, Axon recommends enabling livestream during recording only.

Activation Settings

- **Speed Activation**

This setting determines if the Dual-View camera activates video recording when a specified speed threshold is exceeded. Speed activation is off by default.

- **Speed Reactivation**

Determines if the camera automatically reactivates recording while the vehicle speed remains greater than the configured threshold. When disabled, ending a video while greater than the speed threshold will prevent speed activation until the threshold is exceeded again.

- **Motion Activation**

This setting determines if Fleet cameras automatically transition from Buffering to Event Mode when the Hub detects sudden changes in acceleration that may have been caused by a motor-vehicle accident.

Device Management

- **Body Worn Camera Pairing**

This setting determines if agency Body Worn cameras can be paired with the Fleet 3 system. Pairing allows video review, tagging, upload and settings management of the body-worn camera by the Fleet 3 system.

Evidence Review

- **Evidence Playback**

This setting determines if evidence can be played back in the Dashboard application.

- **Edit Evidence Metadata**

This setting determines if evidence metadata can be edited in the Dashboard application. Metadata includes Evidence Title, Categories, Tags, and ID.

- **Evidence Review Period**

Fleet 3 uploads evidence whenever sufficient internet access is available.

This setting determines the length of time a copy of evidence remains on the Fleet Hub, after recording is stopped, for video playback review and editing metadata.

Meta-data edits from Dashboard during this period overwrite the metadata stored on Axon Evidence.

Upload Settings

- **Wi-Fi Only Upload**

Limits Fleet 3 to only use Wi-Fi for Evidence Upload. It also limits the download of software updates to Wi-Fi. This setting requires coordination with the vehicle router settings. The domain (IP) of <http://fleetevidenceping.com> (52.247.154.57) must only be reachable over the router Wi-Fi interface.

This upload method can overwhelm many Wi-Fi networks. Axon recommends discussing this option with your Axon representative before attempting to use this setting.

- **Priority Upload**

Sets if a user can upload evidence from the system using any connection method available to the Fleet Hub. This setting allows the system to disregard normal routing rules.

- **Power Off Delay**

Sets the Fleet 3 system power off delay. The shutdown timer starts when the ignition sensing wire no longer detects voltage. During a power-off delay, Fleet 3 can record evidence, upload video, and download updates.

The length of time required to upload videos depends upon many factors, such as video quality, length, quantity, and internet bandwidth. Power during the power off delay is supplied by the vehicle battery. Axon recommends a delay length that enables videos from each shift to offload before the system powers down, while taking care to not overly drain the battery.

User Permissions

Note: **Users Can Mute During recording**

This setting controls if your users can use Fleet Dashboard 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**.

- **Users Can Adjust Indicator Light Settings**

This setting determines whether users can adjust indicator light brightness or turn them off.

- **Users Can Use Stealth Mode**

This setting determines whether users can place Fleet 3 into stealth mode. Stealth mode disables visual and audible feedback from Fleet 3 devices. Stealth mode does not affect the Fleet Dashboard.

Fleet 1 & 2 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.

- **Motion 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.