G-CLOUD 15

CROWN COMMERCIAL SERVICES

AXON EVIDENCE DIGITAL EVIDENCE MANAGEMENT SOFTWARE (DEMS) AND ASSOCIATED SOFTWARE APPLICATIONS

SOLUTION DESCRIPTION

RFP Number: RM1557.15

Submitted By: Axon Public Safety UK Limited

ORIGINAL

AXON

TABLE OF CONTENTS

AXON EVIDENCE SOLUTION DESCRIPTION

Managing digital evidence across multiple sources is an operational challenge for modern public safety organisations. From capturing footage in the field to preparing case files, organisations manage large volumes of content under tight timelines and regulatory oversight. Axon Evidence is a secure, cloud-based digital evidence management system that helps organisations streamline each step of the evidence lifecycle—from intake and review to sharing and retention.

Evidence can be ingested from a variety of sources, including Axon body-worn and in-car cameras, third-party systems such as CCTV, and public submissions. Uploads from Axon devices make footage available without extensive manual processes. Evidence from third-party sources, such as CCTV footage or residential doorbell cameras, can be uploaded into the system with automatic file conversion if needed for playback. Digital public evidence submission portals or single-use submission links enable secure community contributions. Additionally, bulk evidence uploads and API integrations can simplify large-scale evidence transfers or recurring data transfers into Axon Evidence.

Tools in Axon Evidence help users quickly locate, organise, and manage digital evidence. Users can quickly retrieve relevant files by filtering search results based on multiple fields, including custom options for flexibility. Integrated playback and annotation allow users to mark key moments and add notes. Investigators can group related evidence within case structures, apply bulk updates to metadata, and use evidence-matching features to confirm that evidence related to an incident is included in a case.

Sharing features support secure collaboration with internal users and external partners. Within an organisation, users can grant tailored access to files so that recipients have only the permissions necessary to view, edit, or share evidence based on their role. External stakeholders, including prosecutors or defense attorneys, can securely receive shared files through a controlled, traceable process.

Axon Evidence enables real-time situational awareness between personnel in the field and command center staff. Location information and live-streaming video give command staff real-time visibility into staff movements and unfolding incidents. Automated alerts notify command staff of critical events—such as a weapon being drawn or a vehicle collision—so they can respond quickly to changing situations.

Axon Evidence helps protect evidence integrity with audit trails, retention policies, and access controls. Actions such as viewing, editing, or sharing are logged in an audit trail to provide a clear and unalterable record of evidence handling without adding manual work. Customisable retention policies help organisations comply with legal and regulatory requirements by automating evidence storage and deletion. Administrators configure role-based access controls to define user permissions across the system so that personnel have the appropriate level of access to evidence, case files, and system settings while protecting sensitive data from unauthorised access.

The system's key capabilities include:

- **EVIDENCE INGESTION** – Facilitates the transfer of evidence from Axon devices and third-party sources, reducing manual effort and simplifying evidence access.
- **EVIDENCE MANAGEMENT** – Organises files with metadata tagging, case-based structures, and automated workflows to simplify evidence management and support proper retention and policy compliance.
- **SEARCH AND PLAYBACK** – Provides advanced search filters, metadata-based indexing, and an intuitive media player for efficient evidence retrieval and analysis.

- **EVIDENCE SHARING** – Facilitates secure sharing of evidence and cases with internal teams or external stakeholders while maintaining chain-of-custody and access controls.
- **CONNECTED FEATURES** – Improves situational awareness and response coordination with live location monitoring, livestreaming video, and automated event recording.
- **AUDIT TRAILS AND EVIDENCE TRACKING** – Safeguards evidence authenticity with tamper-proof audit trails, integrity checks, and comprehensive reporting tools to support chain-of-custody and access controls.
- **CUSTOMISATION AND SETTINGS**– Allows administrators to configure system policies, manage user access, and customise evidence workflows to align with organisational requirements.
- **SYSTEM SECURITY** – Protects evidence with robust security controls at the application level.

SYSTEM ELEMENTS

Axon Evidence relies on hardware and software elements including internet-enabled workstations, mobile devices, and integrated applications. These tools allow users to securely upload, access, and manage digital evidence from various locations. Underlying this system is a cloud-based architecture. Built on a three-tiered structure, the architecture enables secure data ingestion, advanced workflows, structured storage, and reliable access.

The following tables provides a breakdown of the essential hardware and software elements that comprise a standard Axon Evidence deployment. Depending on your desired deployment, other hardware (e.g., body-worn and in-car cameras, interview room equipment, etc.) or software/applications (e.g., Axon programmes that interact with hardware, API protocols, etc.) may be implemented alongside these elements.

HARDWARE

COMPONENT	PURPOSE	LOCATION OR IMPLEMENTATION
Internet-enabled Workstations (Customer-provided)	Allows access to Axon Evidence for evidence management and review; facilitates manual or automatic upload of third-party evidence.	Located in offices, monitoring rooms, or other organisation-authorised locations to connect to Axon Evidence via a web browser.
Internet-enabled mobile devices and tablets (Customer-provided)	Supports in-field evidence capture, upload, and management using Axon applications.	Accessible in the office or in the field.
Axon hardware, such as body-worn cameras, in-car cameras, interview rooms, etc.	Captures evidence and audit activity	Dependent on specific hardware type; may be located in the field, at a station, or in a vehicle

SOFTWARE AND APPLICATIONS

COMPONENT	PURPOSE	LOCATION OR IMPLEMENTATION
Axon Evidence	Provides an interface for managing, reviewing, and	Accessible via secure web browsers on workstations or mobile devices.

	sharing evidence stored in the cloud.	
Axon applications	Allows manual or automatic upload of files from non-Axon (third-party) devices; allows users to complete evidence handling workflows from a mobile device	Depending on the application, may be accessed directly from Axon Evidence on workstations or on mobile devices/tablets.

EVIDENCE INGESTION

Axon Evidence provides flexible ingestion methods that support a wide range of evidence sources, including Axon devices (first-party), non-Axon devices (third-party), and public submissions. Through automated uploads, secure file transfers, and integrations with existing systems, evidence intake is streamlined while maintaining the integrity of evidence files.

The following section outlines the available ingestion methods and how they support reliable evidence transfer.

EVIDENCE INGESTION FROM AXON DEVICES AND APPLICATIONS

Axon Evidence integrates seamlessly with Axon's hardware ecosystem, offering a centralised platform to ingest, organise, and manage evidence securely. Whether from body-worn cameras, in-car cameras, interview rooms, or TASER energy weapons, Axon Evidence simplifies evidence transfer through a variety of flexible methods tailored to meet your needs.

/ AXON BODY-WORN CAMERAS

Axon Evidence supports multiple upload methods for video and audio captured by Axon body-worn cameras. These options reduce manual processes and help provide timely access to evidence in the field and at the station.

- **DOCKING STATIONS –** When a camera is placed in an Axon Dock, recorded footage is transferred automatically to Axon Evidence. This process also clears onboard memory, applies pending updates, and charges the device in preparation for the next shift.
- **AUTOMATIC WI-FI UPLOAD** – Footage can be uploaded over pre-authorised Wi-Fi networks. Once in range, the device begins uploading eligible files without user input.
- **PRIORITY EVIDENCE UPLOAD** – With connected capabilities enabled, critical evidence can be uploaded over LTE for review by authorised personnel. This option supports faster access to footage during ongoing incidents.
- **IN-CAR UPLOAD VIA AXON APPLICATION** – Body-worn camera footage can be uploaded using mobile data computer (MDC) applications while in the vehicle to prioritise faster access and review.

/ AXON FLEET IN-CAR CAMERAS

Axon Evidence supports secure upload of video and metadata captured by Axon Fleet systems. Multiple upload options are available based on vehicle configuration and deployment environment.

- **LTE/4G OFFLOAD** – Axon Evidence accepts uploads from Axon Fleet 3 over LTE/4G networks using an in-car broadband connection
- **WI-FI OFFLOAD** – Axon Fleet 3 can automatically upload evidence to Axon Evidence via Wi-Fi access points, leveraging a Wireless Offload Server (WOS) to manage large data volumes efficiently

/ AXON INTERVIEW

Axon Interview captures video and audio from recorded interviews. Once an interview session is complete, evidence is uploaded directly from the on-premise server to Axon Evidence for long-term storage and management.

/ TASER ENERGY WEAPONS

Axon Evidence receives data from TASER energy weapons that log usage events such as arming, trigger pulls, and cartridge deployments. These detailed, timestamped records support accurate post-incident review and enable organisations to store and organise relevant evidence within Axon Evidence.

/ AXON APPLICATIONS

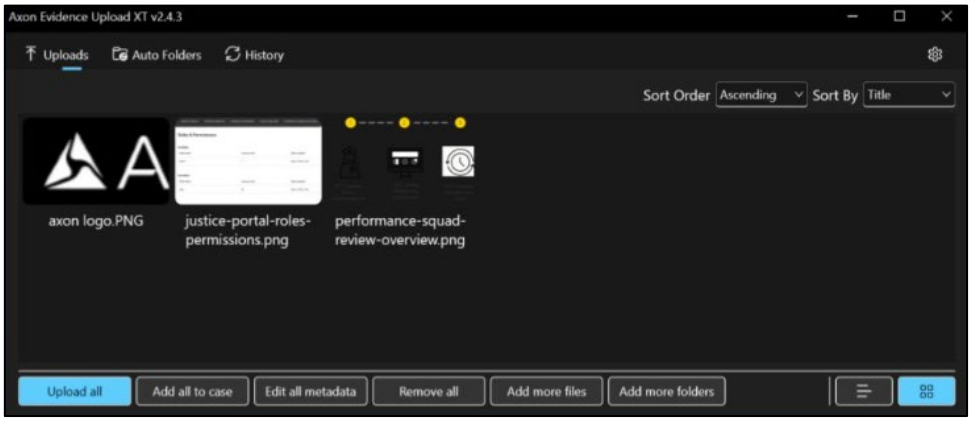
In addition to hardware solutions, our mobile and desktop applications support field-based evidence collection, in-field access to recorded files, and public evidence submissions.

- **MOBILE EVIDENCE CAPTURE** – Personnel can collect and upload photo, video, and audio evidence directly from a smartphone or tablet. Applications allow for tagging, titling, and GPS metadata to be applied so that evidence remains well-organised. Automatic removal of files from the device after upload enhances security.
- **EVIDENCE REVIEW** – Users can access their body-worn or in-car cameras in the field to view live feeds, play back recorded footage, and tag or add metadata.
- **PUBLIC EVIDENCE SUBMISSION** – Secure applications provide secure methods for collecting digital evidence from community members. Requests can be sent to individual community members for file submission via text or email, while public portals allow large-scale evidence intake using shareable links or QR codes. Metadata and chain-of-custody records are automatically applied to maintain evidentiary integrity.

EVIDENCE INGESTION FROM NON-AXON SOURCES

Axon Evidence makes it easy to upload and manage evidence from a variety of non-Axon sources to support system flexibility and integration. Whether uploading individual files from a mobile phone seizure, large datasets from a hard drive or legacy DEMS, or syncing with other systems such as a CAD/RMS, Axon Evidence simplifies the process while maintaining proper organisation and chain-of-custody standards.

- **INDIVIDUAL OR BULK FILE UPLOADS** – Users can upload individual files or large evidence sets to Axon Evidence through web and application interfaces. Files can be organised in bulk using drag-and-drop tools and categorised with relevant metadata. Auto-folder workflows and a command-line tool are also available to support recurring or large-scale uploads.



- **INTEGRATION VIA API** – Axon Evidence uses APIs as a flexible way to integrate with third-party systems and extend evidence management capabilities. APIs support ingestion from other digital evidence management systems (DEMS), enable automated metadata assignment, and allow integration with CAD and RMS platforms for streamlined management.

EVIDENCE MANAGEMENT

Axon Evidence provides tools to help organise, categorise, and manage digital files throughout the evidence lifecycle. These features allow users to assign metadata, group evidence into cases, add investigative notes, apply file retention, and share files with partner organisations. Users can highlight key events within recordings, create clips, and redact sensitive content without altering the original file. Transcription and report-writing tools are available to support documentation workflows. These capabilities help organisations maintain consistency, streamline reviews, and support operational needs during investigations, disclosures, or courtroom proceedings.

The following subsections detail how Axon Evidence streamlines evidence management so that files are well-organised, secure, and accessible when needed.

METADATA

Metadata in Axon Evidence supports file organisation, searchability, and retention. Key metadata fields, such as recording date, device type, and upload source, are applied automatically during ingestion for ease. Users can add or edit fields such as case numbers, organisation-defined categories, or custom tags to support specific workflows.

Administrators can create custom metadata fields to align with organisational needs. This allows Axon Evidence to meet diverse operational needs and local laws and statutes. Three types of custom metadata are available:

- **DROP-DOWN –** Predefined, selectable options to support consistency, such as "Pending Disclosure" or "Disclosure Complete"
- **FREEFORM –** User-entered open text fields, such as case titles or officer names
- **VALIDATED** – Fields with specific formatting requirements, such as structured case numbers

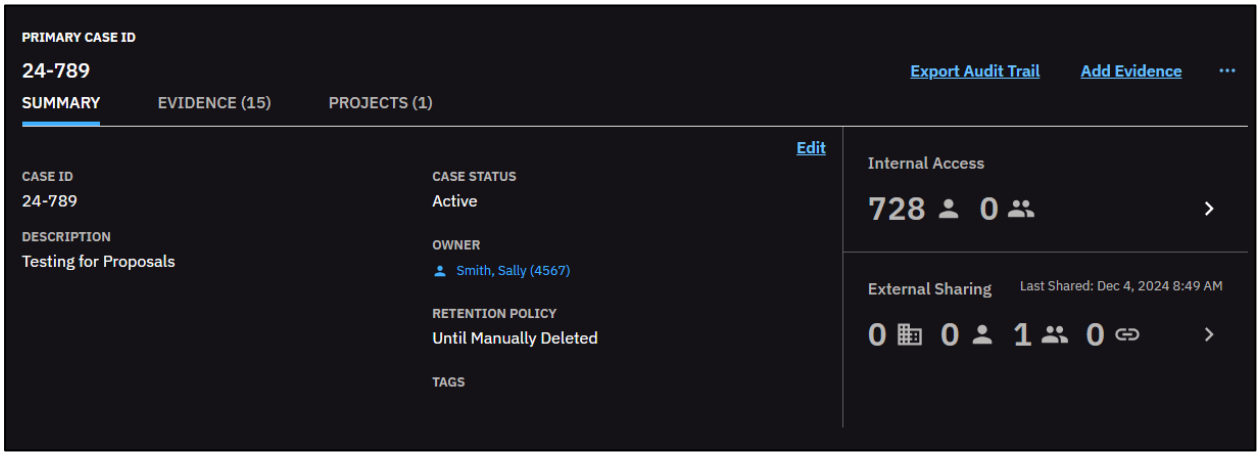
A retention category is an additional type of metadata that determines how long evidence is retained in the system, helping to automatically achieve proper evidence retention. Administrators can create and assign custom categories (e.g., assault, traffic stop, armed robbery) so that evidence is stored for the duration required by law. Once a category's retention date is reached, the evidence is automatically scheduled for deletion. To safeguard

against accidental deletion, a review period allows authorised users to recover files before removal is finalised.

CASES

Axon Evidence allows users to group related files into cases, which function as a virtual container for pieces of evidence that are connected to a single incident or event. Authorised users can create cases to support investigation workflows, disclosure requirements, and proper organisation. Subfolders can be added to further organise evidence and more easily navigate case content, and users can enable notifications to receive alerts when new evidence is added.

Each case includes metadata fields for case ID, title, and description. Files can be added manually or matched automatically based on associated metadata. Administrators can configure default folder templates, retention settings, and access lists to help standardise case management across users and teams.



Within a case, users can:

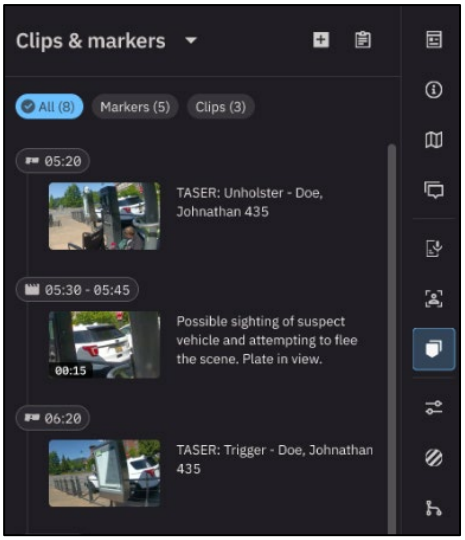
- **REVIEW EVIDENCE** – Access video, audio, image, and document files from a unified view with playback, notes, and annotation features.
- **VISUALISE EVIDENCE LOCATION** – An evidence map displays the approximate location of uploaded content when geolocation is available.
- **APPLY BULK ACTIONS** – Update metadata, modify access, or assign retention settings to multiple files at once.

By offering flexible organisation, secure access management, and intuitive features, Axon Evidence streamlines evidence workflows while maintaining compliance with local policies.

MARKERS AND CLIPS

Axon Evidence includes tools to highlight, extract, and share key moments from video or audio files.

Markers are used to highlight significant events in video or audio files so that users can quickly locate and reference critical moments. For example, an officer can add markers in a video to indicate when a suspect is first observed, when commands are issued, or when force is applied. Markers can be added during recording on an Axon device in the field or within Axon Evidence after upload, whether the video is from an Axon device or a third-party source. Markers can be adjusted, downloaded, annotated, or extracted as standalone image files. Marker reports can also be exported or shared, offering a clear summary of key events in a file for investigators, attorneys, or command staff.



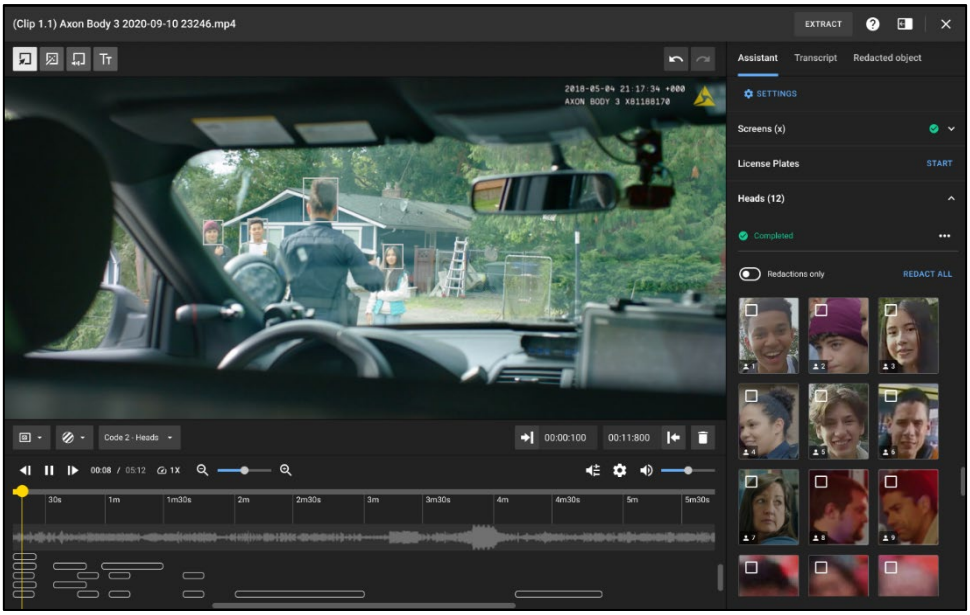
Clips are used to isolate shorter portions of a longer video for targeted purposes like review, redaction, or sharing with external stakeholders. For instance, a prosecutor might request a clip for use in court that shows a suspect's actions prior to arrest. Clips can be extracted as independent evidence files or kept embedded in the original file to preserve context when sharing or disclosing evidence.

Both markers and clips do not alter the original evidence file. Actions are logged in the audit trail to maintain the integrity of the record.

REDACTION FEATURES

Axon Evidence provides tools to redact sensitive content from video, audio, images, and documents while preserving the original evidence file. Tools include the following:

- **MANUAL REDACTION** – Users can precisely control redactions by selecting areas to obscure, mute, or annotate across video, audio, image, and document files.
- **AUTOMATED REDACTION** – Automated tools can assist with common redaction tasks and include object tracking and automated skin blurring options. Users can select between different blur or blackout levels, standard or inverted redaction masks, and audio mask types for further customisation, and can adjust, accept, or remove suggested redactions before saving.
- **AI-POWERED TOOLS** – AI-powered redaction tools detect and redact common elements, such as heads, license plates, and device screens. Up to 20 files can be scanned at once and redaction masks are presented for approval, giving users control over final edits while improving efficiency
- **AUDIO REDACTION** – Audio content can be redacted manually or by selecting flagged words within an Axon-generated transcript. Redacted audio can be muted or a short bleep can be applied. An audio extraction feature also allows users to extract audio from a video file to be stored as stand-alone evidence.



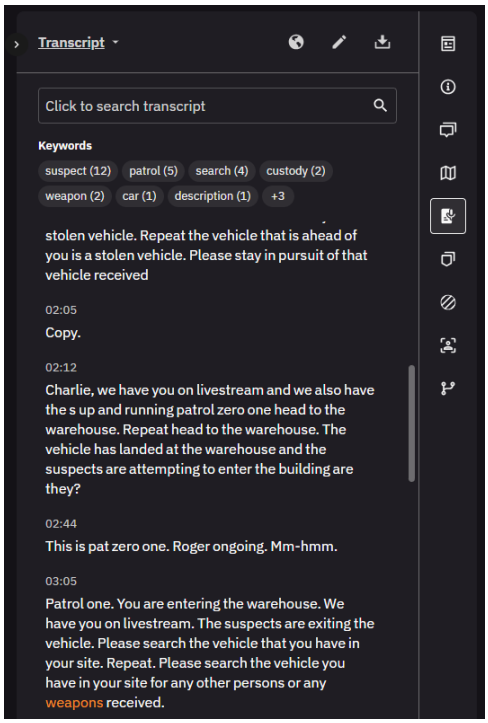
With a combination of manual tools, automation, and AI-powered enhancements, Axon Evidence's redaction features help protect sensitive information, meet compliance requirements, and save valuable time when managing evidence.

AUTO-TRANSCRIBE AND DRAFT ONE

Axon Evidence includes tools to assist with video transcription and report generation. These features are designed to support documentation workflows and reduce time spent on administrative tasks.

Video can be automatically transcribed when uploaded, with the resulting transcript aligned to the video timeline. Axon Evidence identifies common law enforcement-related keywords throughout the transcript, helping users to identify areas that may need redaction or review. Transcripts can be edited, verified, and finalised before being used for case preparation or external disclosure.

Axon Evidence's report writing tool uses AI to create first-draft report narratives directly from transcripts, helping to reduce time spent on paperwork while promoting consistency and accuracy. The generated reports are designed to include placeholders where additional context may be needed, and edits can be made in the simple editing interface. Additional features, such as talk-to-text functionality, provide flexibility. Administrators can configure incident types and draft settings to align with organisational policy.



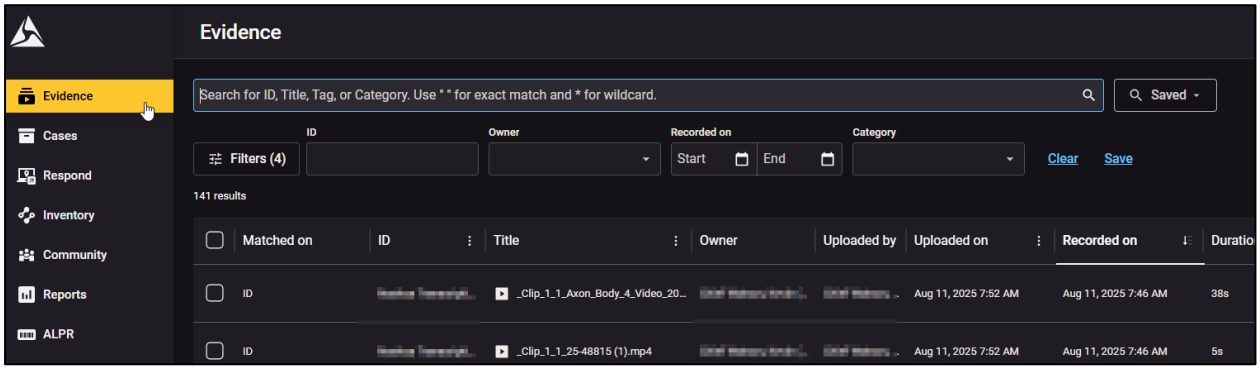
SEARCH AND PLAYBACK

Axon Evidence includes tools to help users locate, review, and analyse files across large volumes of content. Evidence can be searched by metadata, case structure, or file type, and viewed using flexible result layouts. Built-in playback controls support efficient video and audio review, including frame-by-frame navigation, speed adjustment, and metadata overlays. Compatibility with third-party file types allows organisations to centralise evidence management without relying on external conversion tools.

SEARCHING FOR EVIDENCE

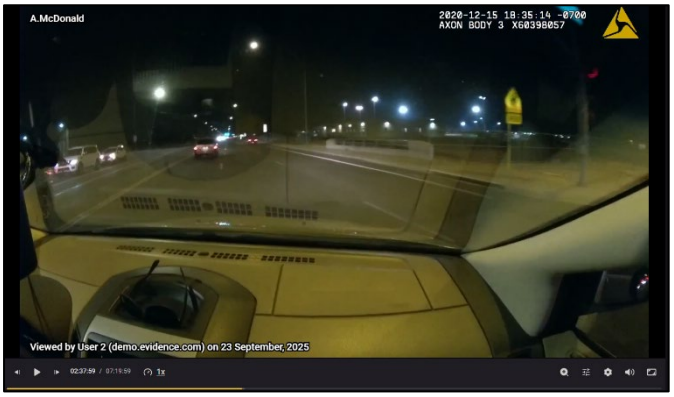
Axon Evidence supports metadata-based search across uploaded files. Search fields include title, ID, category, owner, date, or device serial number. Administrators can also create custom search fields to reflect organisation-specific workflows.

Search results update dynamically as filters are added to provide a responsive search experience. Results can be viewed in list or gallery formats, and users can choose which metadata columns are displayed. Column order can be rearranged, and filters can be used to sort or prioritise results for faster access to relevant evidence. Users can choose to save common searches to save time when completing assigned tasks.



These features help users quickly retrieve specific files during casework, reviews, or disclosure preparation.

PLAYBACK



Axon Evidence includes a built-in media player that supports the review of video and audio files. Similar to widely used media players such as YouTube, the media player includes play, pause, frame-by-frame navigation, and variable speed adjustments ranging from 0.25X to 4X. Users can jump to specific moments using thumbnails or scrub the timeline to navigate longer recordings.

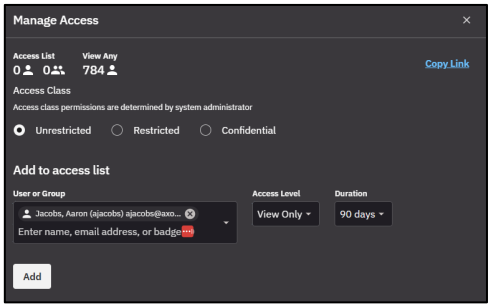
When watching a video, a "Viewed By" watermark appears on the playback screen and includes the username, date, and account URL. This visual indicator enhances accountability, and the viewing action is also captured in the audit trail to provide a record of access. Metadata overlays can also be enabled during playback, and display key information such as recording time, device ID, and assigned user.

THIRD-PARTY PLAYBACK

With native support for an extensive range of file types, Axon Evidence supports built-in playback of video evidence from many non-Axon sources, such as CCTV footage and proprietary video formats. This capability helps law enforcement and legal teams review and store third-party evidence, such as CCTV footage, without requiring external tools.

If a file type is not natively supported, Axon Evidence can automatically convert unsupported file types into a compatible, lossless format for playback while preserving the original file in its native format. Converted files are labeled to indicate playback is not in the original format. If conversion is not possible, organisations can request compatibility assistance through Axon Support.

EVIDENCE SHARING



Axon Evidence supports controlled sharing of digital files or cases with internal users or external stakeholders. Access permissions can be customised by role, case, or file to help align with investigative workflows and disclosure requirements. Sharing activity is logged in the audit trail to support accountability and chain-of-custody documentation.

Axon Evidence provides secure sharing options for both internal and external recipients. Access lists control who can view or interact with files or cases, with configurable settings to restrict access, set sharing durations, and enable or prohibit downloads or resharing. Internal recipients can

simply log in to Axon Evidence to access the shared files. External recipients, such as law enforcement partners, prosecutor's offices, or district attorneys, can log in to their Axon Evidence account to view shared files directly. For those without an Axon Evidence account, a secure login can be created for controlled access.

When a case is shared, recipients receive a separate copy of the case files, which can be independently managed and organised within their account. Case materials such as audit reports, transcripts, and notes can be included with shared files to provide recipients with additional context.

For situations where external users cannot access Axon Evidence, files can be exported as ZIP or ISO packages for sharing via physical media or email. Exported files are password-protected and optional documents such as audit trails or a table of contents can be included to provide a comprehensive view of the evidence.

Sharing actions are logged in the audit trail, providing transparency and accountability by tracking who shared the file, when, and with whom. These features give organisations confidence that evidence is shared securely, meets compliance requirements, and supports collaborative workflows.

CONNECTED FEATURES

Axon Evidence offers connected capabilities that support real-time visibility and improved coordination between field personnel and command staff. These features operate when enabled by device settings and when deployed with Axon hardware with device connectivity/Axon Fusus Plus enabled.

Connected features include the following:

- **LOCATION MONITORING** – Field-deployed cameras and other devices with connected capabilities can report live GPS data. Command staff can view unit locations, monitor ongoing incidents, and assess developing situations through the dynamic map interface.
- **LIVESTREAMING** – Authorised users can access real-time video feeds from actively recording Axon Body 4 or Axon Fleet 3 devices. This feature strengthens operational awareness by giving supervisors a direct view of unfolding events.
- **AUTOMATED EVENT-ACTIVATED RECORDING** – Certain in-field actions, such as drawing a weapon or activating emergency equipment, can automatically initiate a camera recording and provide command staff with a notification in Axon Evidence.
- **MOBILE ALERTS** – Supervisors can receive push notifications and real-time updates via the Axon Evidence mobile app. Notifications include activity such as weapon draws, vehicle events, and triggered recordings.

AUDIT TRAILS AND EVIDENCE TRACKING

Axon Evidence supports a proper chain of custody by logging system activities—including actions related to evidence access and playback, user activity, and system changes—in tamper-resistant audit trails. Audit trails cannot be edited or deleted, even by administrators, and each entry includes essential details such as the date, time, user information, and a description of the activity performed.

Available audit trails include:

- **ORGANISATION AUDIT TRAIL** – Organisation-wide administrative changes to settings, policies, and accounts.

- **EVIDENCE AUDIT TRAIL** – Actions for individual pieces of evidence, such as viewing, editing metadata, sharing, or redacting. Includes details such as associated IP addresses and SHA-2 hash values for verifying file integrity.
- **CASE AUDIT LOG** – Updates to a case, including metadata changes, external sharing, and the addition of new evidence or users to access lists.
- **USER AUDIT TRAIL** – Actions performed by a specific user, such as login attempts, evidence viewing, and initiating redactions or deletions.
- **GROUP AUDIT TRAIL** – Group-related activity, including creation, membership changes, and permission updates.
- **DEVICE AUDIT TRAIL** – Device-specific actions, such as registration, status changes, and metadata updates. Depending on the type of device selected, additional information may be included, such as the remaining battery percentage, remaining storage, and firmware version.
- **AXON RESPOND AUDIT TRAIL** – Activity related to Axon Respond, including livestream access, map usage, and notifications.
- **COMMUNITY REQUEST AUDIT TRAIL** – Activity associated with evidence submitted through Community Request or Community Request+ portals, including invitation creation and evidence triage.

Administrators and authorised users can generate and download these audit trails to support investigations or compliance monitoring. Most audit trails are available in PDF format, while some, like user and device audit trails, can also be exported as CSV files for sorting and analysis. Axon Evidence allows users to specify custom date ranges or use preset timeframes to tailor the scope of the reports to their needs.

CUSTOMISATION AND SETTINGS

Axon Evidence offers a range of administrative controls that allow administrators to configure system functionality, user access, device settings, and security policies to align with operational needs. The following section explores the key customisation options available in Axon Evidence.

ORGANISATION SETTINGS

Administrators can tailor Axon Evidence's functionality and structure to align with organisational policies and operational needs. Key configurable elements include:

- **RETENTION CATEGORIES** – Each retention category is set up with a name for classification and a retention period, which can be defined in days, weeks, months, or set to manual deletion. Categories also include access restriction settings, determining whether files are accessible to users with proper permissions or restricted to only users with advanced clearance.
- **ROLES AND PERMISSIONS** – Organisations can create an unlimited number of custom roles to control access rights across the system. Permissions can be applied to individual users or groups to control what actions are available, such as viewing, editing, redacting, or sharing files.
- **CASE SETTINGS** – Configures case retention and templates, evidence matching settings, notification, and workflows for consistency in case management.

Other available organisation settings include custom metadata, evidence playback preferences, and redaction settings, allowing organisations to further customise the system.

USER SETTINGS

Administrators have comprehensive control over user creation, password settings, and overall user management so that access to evidence and system functions is secure, role-based, and aligned with organisational policies.

- **USERS** – Users can be added manually or imported via Active Directory (AD).
- **GROUPS** – Users can be organised into groups to simplify access management. Group permissions apply to each member and can be managed locally or through AD synchronisation.
- **COMMAND HIERARCHY** – A hierarchical structure can be applied to reflect reporting relationships and access levels across teams or divisions. This setting supports structured access workflows based on operational roles.

DEVICE SETTINGS

Axon Evidence gives administrators comprehensive control over the configuration and management of Axon hardware. Note that depending on your deployment, certain device settings may not be applicable.

- **DEVICE SETTINGS** – Device settings include recording settings, video quality, and audio settings. General settings apply across the board so that devices are customised to meet operational needs, such as adjusting recording quality or enabling stealth mode for covert operations.
- **ROLE-BASED SETTINGS** – In addition to standard device settings, administrators can configure devices based on user roles. For example, patrol officers may have different recording settings than investigators or supervisors.
- **DEVICE HOME** – Assigns devices to specific locations, such as precincts or storage facilities, to simplify inventory tracking when devices are not in use.

SECURITY SETTINGS

Axon Evidence includes configuration options that allow administrators to manage system access and align usage with organisation policies.

- **SIGN IN CONFIGURATION** – Login settings can be customised to enforce password complexity, set session timeouts, and limit failed login attempts.
- **MULTI-FACTOR AUTHENTICATION (MFA)** – MFA strengthens user authentication by requiring a second layer of verification during login and is required by Axon Evidence. Administrators can configure available MFA methods, including mobile apps, text messages, email, or automated calls. For added flexibility, users can select their preferred authentication method.
- **API** – API integrations can connect third-party applications and services to Axon Evidence. Administrators can control API access permissions and monitor usage.
- **SINGLE SIGN-ON (SSO)** – SSO can be configured using the organisation's existing authentication system.
- **IP ADDRESS RESTRICTIONS** – Access can be limited to specific IP ranges to prevent unauthorised use outside approved networks. Exceptions may be configured for Axon mobile applications.

SYSTEM SECURITY AND ARCHITECTURE

Axon Evidence is delivered as a Software as a Service (SaaS) platform hosted on Microsoft Azure's trusted cloud infrastructure. The system is designed to support secure digital evidence management by applying protections across each layer of the platform—from ingestion to storage and access. Evidence is encrypted in transit and at rest, segmented logically by tenant, and protected by role-based access controls and comprehensive audit

trails. The platform architecture supports high availability, disaster recovery, and compliance with public safety requirements.

Together, these features help organisations to maintain evidence integrity, enforce chain of custody, and meet data security expectations in high-trust environments.

ARCHITECTURE AND DESIGN

Axon Evidence runs on a secure cloud system where each organisation has its own private space. Even though many organisations use the same system, their data is kept separate and cannot be seen by others unless they choose to share it. Each tenant is isolated and protected through application-level security controls and session enforcement. Axon manages and deploys Axon Evidence within Microsoft Azure's infrastructure, using virtualised compute, object storage, and built-in resiliency services to support availability, redundancy, and performance.

Evidence data and application states are replicated synchronously within Azure regions and backed up in geographically separate, fault-tolerant storage locations. This structure supports business continuity, helps maintain platform stability, and eliminates single points of failure.

In addition, Axon Evidence uses a three-tiered cloud architecture to separate evidence ingestion, processing, and storage functions. This design supports consistent performance under increasing data volumes, simplifies feature deployment, and helps critical tools—such as transcription, redaction, and audit reporting—to operate without delay.

The roles of each tier include:

- **TIER 1: SECURE ENTRY POINT** – Incoming data from connected devices and authenticated users is encrypted in transit and routed through a secure entry point. This layer validates sources before allowing data into the system and applies protective protocols to prevent unauthorised interaction and access.
- **TIER 2: APPLICATION AND DATABASE** – The application layer supports evidence categorisation, metadata tagging, search and playback, and case management. Features such as transcription, redaction, and automated alerts operate within this tier.
- **TIER 3: EVIDENCE STORAGE** – Axon Evidence stores digital evidence in encrypted cloud environments built on Microsoft Azure. The platform supports scalable storage allocation and centralised retention configuration without requiring organisations to maintain on-premises infrastructure.

DATA SECURITY AND ENCRYPTION

Security controls are built into Axon Evidence to help protect sensitive data and system access. Security measures include the following.

- **ENCRYPTION IN TRANSIT –** Data in transit is protected using Transport Layer Security (TLS) 1.2 with 256-bit encryption and Perfect Forward Secrecy. Connections are authenticated and encrypted before transmission.
- **ENCRYPTION AT REST –** Stored data is encrypted using AES-256 in alignment with NIST and CJIS requirements. FIPS 140-2 validated cryptographic modules are used to support compliance and security expectations for public safety environments.
- **ACCESS CONTROLS –** Access to Axon Evidence is managed through role-based access controls (RBAC), evidence-level access lists, and support for Single Sign-On (SSO) via SAML. Multi-factor authentication (MFA) is required and can be configured with options such as authenticator apps, SMS, or email.
- **MONITORING AND DETECTION –** Axon's Security Operations team uses centralised Security Information and Event Management (SIEM) tools to monitor for potential threats. Incident response procedures follow ISO/IEC 27001, SOC 2, and CJIS standards, with rapid escalation and notification processes in place.

COMPLIANCE MEASURES

Axon Evidence is developed and operated under a robust information security programme designed to align with legal, regulatory, and contractual standards relevant to public safety organisations.

- **CERTIFICATIONS AND AUDITS –** Axon maintains third-party certifications including ISO/IEC 27001:2022, SOC 2 Type 2, ISO 27017 (cloud controls), ISO 27018 (data privacy), and ISO 27701 (PIMS). The solution is aligned with the FBI's CJIS Security Policy and FedRAMP High standards for customers in the United States
- **AUDIT TRAILS –** User actions, such as file access, metadata edits, redactions, and sharing, are captured in tamper-resistant audit logs. These logs cannot be deleted, even by administrators, and remain available even after the evidence has been removed from the system
- **BUSINESS CONTINUITY AND RECOVERY –** Axon has developed an Information System Contingency Plan (ISCP) for Axon Evidence in accordance with NIST SP 800-34. In the event of a regional data center failure, Axon Evidence can be restored in a secondary Azure region with a target Recovery Time Objective (RTO) of less than 24 hours and asynchronous evidence replication within 15 minutes of creation
- **PHYSICAL AND ENVIRONMENTAL CONTROLS –** Microsoft Azure data centers are monitored 24/7 and protected by biometric access, perimeter fencing, and video surveillance. Facilities are designed to withstand environmental and physical threats and are SSAE 16 and ISO 27001 certified

AXON AI ERA PLAN

The Axon AI Era Plan is a bundled offering that brings together Axon's current and future AI-powered tools under a single procurement. Designed to help support operational efficiency, evidence processing, and administrative workflows, the plan includes all available AI features today-along with access to upcoming capabilities as they are released.

Each solution in the plan is developed to integrate into existing public safety workflows, helping organisations manage audiovisual evidence, streamline documentation, and support informed decision-making while helping better manage administrative tasks and community interactions. By consolidating AI solutions into one scalable plan, organisations can reduce procurement complexity, support long-term planning, and deploy AI more consistently across operational units.

Tools included in the AI Era Plan are designed to help:

- Automate transcription, create first-draft reports, and summarise audio from video evidence.
- Support multilingual operations and real-time communication.
- Accelerate workflows by combining image collection and data extraction, streamlining image review, video analysis, and form population.
- Provide policy guidance through secure, AI-powered search.

The AI Era Plan reflects Axon's continued commitment to responsible innovation—grounded in officer feedback, field-tested design, and ethical oversight. With a focus on real-world use, the plan is intended to help organisations adopt AI tools that support—not replace—officer expertise.

AXON AI ERA PLAN FEATURES

*Please note that the availability and timing of AI features described in this plan are subject to change. Axon's product roadmap is continuously evaluated and may be adjusted based on technical considerations, customer feedback, and evolving operational needs.

FEATURE NAME	DESCRIPTION
Unlimited Auto-Transcribe	Generates automated, searchable transcripts from video and audio recordings to support documentation and case review.
Draft One	Produces structured first-draft incident reports using body-worn camera transcripts.
Unlimited Smart Detection	Automatically detects human forms within body-worn camera footage.
Evidence Translation	Will allow transcript translation between English and Spanish within Axon Evidence to support multilingual casework.
Form One	Will auto-fill common organisation forms using structured data from transcripts to help reduce manual entry.
Brief One	Will generate summaries from transcripts to help highlight critical information.
Axon Body 4 Live Translation (Axon Assistant Feature)	Will provide real-time spoken language translation through Axon Body 4 to support communication in the field.
Smart Capture	Will extract structured ID and license plate data to support documentation and case records.
Attribute Search	Will allow users to search video content based on descriptive terms such as clothing or carried items.
Policy Chat	Will provide secure, AI-powered responses to organisation-specific policy questions within Axon Evidence.

CAPTURE TRUTH
ACCELERATE JUSTICE
PROTECT LIFE

AXON