SOLICITATION 766-11825

INTEGRATED BODY WORN CAMERAS AND DIGITAL EVIDENCE MANAGEMENT SYSTEM FOR THE FORT LAUDERDALE POLICE DEPARTMENT

TECHNICAL PROPOSAL

Submitted by:

TASER International, Inc.

17800 North 85th Street
Scottsdale, AZ 85255
800.978.2737

October 28, 2016

October 26, 2016

Adam Makarevich
Procurement Specialist II
City of Fort Lauderdale, Procurement Services Division
100 North Andrews Avenue
City Hall, Room 619
Fort Lauderdale, Florida, 33301

Dear Mr. Makarevich:

In response to the City's Request for Quote (RFQ), TASER International, Inc. ("TASER") is enclosing information to assist the Fort Lauderdale Police Department ("FLPD") with researching body-worn cameras and an evidence storage and retrieval system.

The attached proposal provides evidence of the suitability of Axon body-worn cameras for the FLPD and a framework for potential implementation. TASER's future-oriented technologies will help your officers focus on policing; from capture to courtroom, the Axon platform lets you follow the progress of a case, organize your data, and share your records.

The TASER team has worked diligently for years in developing and deploying sustainable body-worn camera programs that make a difference to all stakeholders involved – the officer, supervisor, administrator, prosecutor, and citizen. It is the company's intention to evolve this work for years to come in collaboration with law enforcement agencies throughout the world. TASER is a proven vendor with industry leading experience and operations that have been deployed at scale. More than 5,000 agencies, 100,000 users and 35 Major Cities are deployed on Axon and Evidence.com.

TASER's innovative Axon law enforcement technologies provide protection for officers while improving accountability, and enhancing transparency. Evidence.com turns what was once an overwhelming amount of information into a searchable database. In addition to automatically ingesting videos generated from Axon cameras, in-car videos, digital photos, audio recordings, PDF files, etc. can all be managed in Evidence.com. The platform features robust searching, categorization and retention capabilities, redaction tools, and simple, secure methods of sharing evidence with partner agencies, Prosecutors and District Attorneys.

In additional to the following features, the Axon and Evidence.com ecosystem provide seamless management of digital evidence.

- **Streamlined Workflow** - From capture to courtroom, securely share and track digital evidence across public safety stakeholders
- **Field-Ready Smart Devices** - Use Bluetooth and Wi-Fi to better track, manage, and enable body-worn cameras and in-car video
- **Centralized Management** - Keep all your data in one place with our centralized and scalable cloud-based system
- **Audited And Verified** - Record every interaction with any piece of digital evidence
- **Secure Data** - Trust our industry–leading people, practices, and products that comply with security standards like CJIS and ISO 27001

If you have any questions regarding the information enclosed, please contact the following TASER personnel.

Julia Leibelshon, Sr. Proposal Manager 17800 N. 85th Street Scottsdale, AZ 85255 (P) 480-502-6249 (F) 480-905-2000 jleibelshon@taser.com TASER.com, Axon.io	Andrew Grayson, Axon National Director 17800 N. 85th Street Scottsdale, AZ 85255 (P) 602-350-8111 (F) 480-905-2000 agrayson@taser.com TASER.com, Axon.io

We look forward to the next stage of the process and thank you for your consideration of TASER's responses.

Sincerely,

Joshua Isner
Executive Vice President, Global Sales

TABLE OF CONTENTS

Tab 10 Supplemental Information

A. Axon Body 2 Product Specifications
B. Axon Body 2 Dock Product Specifications
C. Axon Flex 2 Product Specifications
D. Evidence.com Product Specifications
E. Evidence.com for Prosecutors Product Specifications
F. Evidence Sync Product Specifications
G. Axon Signal Product Specifications
H. Axon View Mobile Application Specifications
I. Axon Capture Mobile Application Specifications
J. CAD/RMS Product Specifications
K. Professional Services Offerings
L. Detailed Redaction Overview
M. Evidence.com Administrator Guide

TABLE OF CONTENTS

EXECUTIVE SUMMARY

After reading the RFQ, we interpreted that your primary objectives are to obtain a turn-key solution including reliable point-of-view body-worn cameras, a digital evidence management system complete with accessories and ancillary components.

The Axon and Evidence.com suite is end-to-end and will offer management of your evidence from Capture-to-Courtroom. Every product – from our Smart Weapons, to our body-worn cameras, to our digital evidence management system – integrates seamlessly with the other products and often complements the systems and processes you already use.

Footage is uploaded automatically while the camera charges and data can be quickly shared by sending a link. The platform lets you follow the progress of a case, organize your data, and share your records. FLPD will save hours on manual processes; and because TASER's digital evidence management system is cloud-based, FLPD can adopt video technology immediately without building a new infrastructure.

TASER is committed to providing a comprehensive, end-to-end solution for capturing, transmitting, managing and storing video that will surpass the FLPD's expectations and protect its officers, department and City for years to come. TASER's proposal provides evidence of the suitability of its Axon body-worn cameras for the FLPD and a framework for its potential implementation.

THE #1 ON-OFFICER VIDEO PLATFORM

AXON CAMERAS ARE BUILT FOR LAW ENFORCEMENT

TASER has a proven track record of successfully implementing and supporting body-worn video programs for agencies of all sizes. TASER's ability to instantly scale its offerings to agencies of any size, along with its unparalleled implementation and post-sale support services, explain why 95% of the major U.S. agencies deploying body camera programs have chosen TASER's Axon cameras and evidence management suite. TASER is uniquely suited to meet the end-to-end requirements of the FLPD, today and as the agency's needs evolve.

The Axon system represents an ultra-durable, body-worn camera system designed to balance simplicity and performance through the following features:

- **PRE-EVENT BUFFER -** The timing of incidents is unpredictable. With a pre-event buffer feature, officers will not miss a critical moment if the camera has not yet been activated at its outset. Officers can capture the entire story including build up, not just the incident itself.
- **DURABLE DESIGN -** Officer equipment must hold up in the heat of the moment and the cold of winter. TASER cameras can withstand extreme conditions and the toughest days.
- **SIMPLE DOCK-AND-WALK -** At the end of officers' shifts, our technology goes to work, automatically uploading digital evidence to the cloud. Axon devices also simultaneously recharge in the dock to ensure they are ready for the next shift.
- **MOBILE APPS -** Axon cameras come with a mobile application that allows officers to stream, tag, and replay videos in the field for easy searchability later.
- **RETINA LOW-LIGHT -** Most incidents do not occur in broad daylight. With TASER low-light technology, the camera automatically adjusts to changes in lighting, functioning like the human eye.
- **A COMPLETE VIEW -** Axon Flex features point-of-view mounts that give an officer's perspective. Axon Body features a wide-angle lens to capture more of what you see. With either choice, you'll see it all.

DIGITAL EVIDENCE MANAGEMENT

EVIDENCE.COM: THE BEST WAY TO HANDLE DIGITAL EVIDENCE

Whether collecting, transferring, managing, retrieving or sharing evidence, Axon's "dock and walk" workflow improves the process and reduces the day-to-day burden on officers, saving timely and expensive man-hours. With the Axon Dock, videos from Axon cameras are automatically and securely transferred to Evidence.com, TASER's cloud-based storage solution, during routine charging. TASER also provides features enabling the FLPD to easily and securely connect with its partners, from city officials, to neighboring agencies, to the City's prosecutor offices.

High quality, accessible information helps agencies save valuable time and resources, allowing greater focus on the agency's most important priorities. TASER provides the following features and functionality to achieve this goal:

- **LARGE AGENCY SUPPORT -** Manage large deployments with Active Directory integration, operational group permissions and enterprise-level reporting.
- **SECURITY -** Protect the evidentiary value of agency data with CJIS-compliant storage, encryption, multi-factor authentication and real-time threat detection.

- **AUDIT TRAILS -** Prove chain of custody of evidence and review actions taken by users across Evidence.com.
- **INTEGRATIONS -**Increase user compliance, saving time and expenses with features such as automatic metadata tagging and automated retention schedules based on the FLPD’s CAD/RMS.
- **ASSISTED REDACTION -** Streamline FOIA requests by automating the video redaction process.
- **FILE SUPPORT -** Manage multiple digital evidence formats, including body-worn video, in-car video, interview room video, CCTV, photographs, audio, documents, and more in one place.
- **PROSECUTOR EDITION -** Share evidence seamlessly using the industry's only scalable solution for prosecutors.

Background

TASER’s mission is simple: **protect life and protect truth**. TASER provides body-worn cameras to Law Enforcement, and has been providing these services for 9 years. Founded in 1993, we first transformed law enforcement with our conducted electrical devices. Today, we continue to define smarter policing with our growing suite of technology solutions, including Axon body-worn video cameras and Evidence.com, a secure cloud-based digital evidence management platform.

TASER incorporated on January 5, 2001 in Delaware as TASER International, Inc. In May 2001, TASER became publicly traded on the NASDAQ stock exchange (TASR).

As a business unit of TASER, Axon builds on a history of innovation in policing. Axon creates connected technologies for truth in public safety, and our hardware and software solutions are built specifically for law enforcement. Axon is not just a collection of individual technologies; it is a cohesive ecosystem. Every product works together, built by the same team of engineers and supported by the same technicians.

Main Office and Service Locations

TASER’s corporate headquarters and manufacturing facility are located in Scottsdale, Arizona with an additional state-of-the-art office in Seattle, Washington. Professional Services staff are based out of various locations across the United States and travel as necessary.

The FLPD will be serviced from the following TASER locations:

TASER Headquarters
17800 N. 85th Street
Scottsdale, AZ, 85255
TASER.com

TASER Axon Washington
1100 Olive Way, Suite 1300
Seattle WA 98101
Axon.io

Officers and Principals / Key Staff

TASER's project team is comprised of individuals with experience in law enforcement and in supporting our law enforcement partners worldwide. Our most experienced and skilled personnel will be involved in the implementation, development, deployment, management, and support of the FLPD's body-worn camera and digital evidence management program. With more than 154,000 cameras in the field, TASER has the experience to evaluate the FLPD's unique situation and deploy personnel as necessary. The FLPD will have access to TASER's personnel throughout the life of the project to ensure that the FLPD's deployment is completed successfully and on time.

The following TASER personnel may be involved in some part of the demonstrations, pilot, implementation, set up, follow up and support of your Axon and Evidence.com program. All of these individuals, and others, work together to be an unbeatable team when it comes to the implementation of Axon cameras and Evidence.com including the day to day service and support expected by the FLPD.

TASER Regional Support Management Team

The Regional Support Management team's primary purpose is to ensure good standing health for the FLPD's Axon and Evidence.com program, and providing the necessary resources needed to make sure agencies are set up for success. The Regional Support team members accomplish their mission utilizing consistent communication and can be reached 24 hours a day, 7 days a week.

TASER's Regional Support Managers act as primary points of support for customers to ensure positive and successful engagement with their Axon & Evidence.com deployment. As an expert on all Axon products & services, your Regional Support Manager will uncover and maintain an understanding of your goals, pain points, and drivers to improve your agency's customer experience. As updates and features are released, your Regional Support Manager will troubleshoot all changes to ensure a successful experience for customers.

The following TASER personnel will be available to lead the implementation, set-up, follow-up and support of your Axon and Evidence.com program for **Phase II – Pilot Program (Deployment).**

Chris Baker, Sr. Regional Support Manager

Chris is the Sr. Regional Support Manager and supplemental point of contact within TASER headquarters. In addition to managing the Regional Support team, his job is to ensure a good standing health for your agency's Axon and Evidence.com program by utilizing consistent communication, virtual support, and providing the necessary resources needed to make sure you are set up for success. Chris has been with TASER since January 2013 and is also the Regional Support Manager for the Southeastern US, including Florida, Georgia, North Carolina and Alabama. He is based out of TASER HQ in Scottsdale, AZ.

Pre-Sales System Engineers

TASER's Pre-Sales System Engineers are subject matter experts in the area of Software as a Service (SaaS), embedded systems, and networking, leveraging TASER International's Evidence.com and Axon body-worn camera systems. As members of the TASER sales team, the Sales Engineers support the campaign to provide on-officer evidence capture devices and SaaS solutions to more than 15,000 police departments in the United States and abroad.

Uriel Halioua, Senior Pre-Sales System Engineer

Uri is a Subject Matter Expert ("SME") on body-worn video, digital evidence capture devices, and TASER's Axon body-worn video cameras as well as Evidence.com and other forms of digital evidence management. He conducts customer site assessments, including network, electrical, and physical assessments. He also provides pre-sales engineering support to both the domestic and international sales teams.

TASER Professional Services Team

In the past 12 months, TASER's experienced Professional Services Team has completed over 211 deployments and has conducted 830 trials and evaluations.

The following TASER Professional Services personnel will be available to lead the implementation, set-up, follow-up and support of your Axon and Evidence.com program for **Phase III – Additional Purchase (Anticipated Full Deployments).**

Charles Foster, Lead Manager, Technical Services

Charles first started at TASER International in March 2004 in the IT Department and advanced to National Field Services Manager until he left the company in 2009. During his previous tenure with TASER, Charles was involved in implementing countless CEW programs both domestically and internationally as well as assisting in creating and teaching the Technical Services and Investigations Course formerly known as the Armorer's Course. He holds a Bachelor of Science in Network and Communications Management from DeVry University, has been in the Military since 2010, and is currently a First Lieutenant in the United States Army Reserve. Charles is based out of TASER headquarters in Scottsdale, AZ.

CHRISTOPHER BAKER

480-463-2130 · cbaker@taser.com

PROFESSIONAL EXPERIENCE

TASER International

Senior Regional Support Manager September 2016-Present

- Manage team of Regional Support Managers (RSM) to ensure world class training and support on the Axon video system and Evidence.com
- Implement processes and procedures for RSM team to accomplish team and company objectives
- Manage the success of trial Evidence.com programs at police departments and sheriff offices in the Southeast Region.

Regional Support Manager January 2013-September 2016

- Direct the implementation of AXON video system and EVIDENCE.com digital evidence maintenance software program in over 175 police departments and sheriff's offices in 22 states.
- Report status and condition of current customers directly to company executives.
- Gather feedback from law enforcement officers from across the country and work directly with product developers to improve existing products.

Phoenix Suns

Game Night Basketball Communications Staff October 2009 – April 2014

- Train new Game Night Communication Staff members.
- Record and transcribe interviews with players and coaches.
- Collect and compile team statistics.
- Create and distribute statistical information packets that are distributed to all 30 teams along with local and national media.
- Direct interaction with Suns and visiting players as well as local, visiting, and national media.

Phoenix Mercury

Basketball Communications Assistant March 2010 – April 2012

- Managed and directed the Game Night Communications Staff as well as the Al McCoy Media Center and press room during over 50 Phoenix Mercury games.
- Trained new Game Night Staff members.
- Created and edited team Media Guide and team Postseason Guide.
- Analyzed statistics to determine trends and tendencies as well as updated, tracked, and distributed team statistics and trends.
- Facilitated press conferences between home and visiting teams with ESPN.

INTERNSHIP EXPERIENCE

Wealth Management Intern,

Merrill Lynch, Mesa, AZ Summer 2012

- Researched over 100 different companies, bonds, and mutual funds for company information, levels of potential risk, historical returns, and related current events to determine potential new investment opportunities and reported assessment and possible strategies to a Merrill Lynch Vice President.
- Participated in daily brainstorming exercises to think of creative ways to fix everyday problems and create new business solutions.

VOLUNTEER WORK

Hospice of the Valley; Patient Volunteer March 2012 - Present

- Visit and provide emotional and physical aid to terminally ill patients on a weekly basis.

EDUCATION

Bachelor of Science; Finance **Graduation: December 2012**

W. P. Carey School of Business at Arizona State University, Tempe, Arizona **GPA 3.71**

Dean's List

Uriel Halioua

602-820-5408
uri@taser.com

Experience

Pre-Sales Systems Engineer

TASER International - August 2009, Present

I travel across the nation and internationally providing pre-sales support to TASER International's sales team. My role is to provide product presentations, answering technical Q&As, assessing customer capabilities and needs, and making customers fall in love with the cloud.

- Subject Matter Expert (SME) pertaining to EVIDENCE.COM and other forms of digital evidence management.
- Subject Matter Expert (SME) on on-body video, digital evidence capture devices, and TASER's AXON Flex On-Officer video capture device.
- Evangelizes EVIDENCE.COM and TASER video capture solutions.
- Evangelizes Cloud Computing and Software As A Service (SAAS) to the Law Enforcement, Federal, and Military Markets.
- Supporting TASER's Weapons and Video Evidence Sales teams in pre-assessment and closure of business opportunities.
- Engaging with technology decision makers (Chiefs of Police, Command staff, Sheriffs, Directors of IT) through technical sales presentations, solution demonstrations, technical workshops, competitive displacement, and exploratory discussions.
- Assisting in RFP/RFI responses.
- Development of custom Video Evidence solutions that do not exist within present product offering to customer’s requirements and objectives.
- Documented customer feature requests and issues, providing feedback to sales and product management.
- Presenting TASER’s technical & business value proposition at industry events.
- Transfer of industry, technical, and product knowledge to customers and colleagues.
- Proactive planning to prevent post sales issues that shorten time to revenue.
- Close interaction with product and project management to ensure development coincides with the growing needs of the customer.
- Conducting customer site assessments. This includes network, electrical, and physical assessments.
- Sole sales engineer providing pre-sales support to entire domestic and international sales teams.

System Deployment Engineer

BroadSoft - January 2008, June 2009

- Ensure the successful installation, integration, and deployment of our products in customer environments while maintaining quality and superior customer satisfaction.
- Provide technical training and product overview.
- Execute an Acceptance Test Plan with a customer representative.
- Correspond with sales engineering and product management during the installation phase.
- Identify design issues, create problem reports, and follow up with customer for resolution.
- Coordinate and execute customer upgrades.

Network Operations

Primus Telecommunications - January 2004, December 2007

- NOC Monkey

Network Operations Specialist

Sprint - January 2000, January 2003

Tech Support

RCN - January 1998, January 1998

Charles W. Foster II

(602)571-3432
cfoster@taser.com

Career Objective

Seeking a responsible position with a world class organization that will allow me to utilize my vast experience and training

Professional Profile

- Provided subject matter expertise for customer and technical support to law enforcement agencies and Military for advanced TASER products. This included product maintenance, problem-solving, trouble-shooting, and implementing proactive procedures and systems
- Recognized and sought after expert in problem-solving and troubleshooting advanced technical products
- Initiated customer and technical support practices across technical and product areas
- Planned, organized and implemented proactive procedures on advanced TASER systems
- Managed training and supervision of customer and technical support personnel
- Led 41 Military Police soldiers and 1 Combat Medic during combat operations in Kabul, Afghanistan

Professional Experience

TASER International, Scottsdale, AZ — *09/2016 – Present*

Lead Manager, Technical Services

- Manage Professional Services Managers who perform on-site professional services including training, best practices and work flow creation
- Train, motivate, counsel and monitor the performance of all Professional Services Managers and consultant staff
- Manage all Professional Services Managers to ensure that customers are retained, satisfied and that their needs are fulfilled

Professional Services Manager — *08/2014 – 09/2016*

- Contributes recommendations to strategic plans and reviews, prepares and completes business plans, implements best practices for all TASER CEW and AXON products
- Maintain contact with customers, visits operational environments, conducts training, benchmarks best practices, and analyzes information and applications
- Studies, evaluates and re-designs Professional Services programs related to TASER CEW and AXON products
- Provides a level three support resource and technical advice to resolve issues related to all TASER CEW and AXON products as well as diagnosing client network problems

Appointment-plus, Scottsdale, AZ — *05/2012 – 8/2014*
Major Account Manager

- Responsible for maintaining high level of major account retention by providing world class customer service
- Research and compile major account information and recommend standardization and functionality to client
- Coordinate with high level executives to facilitate account upgrades and grow Enterprise solutions
- Serve as liaison between major account clients and internal departments to include sales, client services, information technology and accounting
- Research, compile and reconcile critical major account information in order to maintain good standing with client base

Employbridge, Inc., Phoenix, AZ — *03/2010 – 05/2012*
Account Manager

- Secure new accounts and expand business in existing accounts
- Prepare and present proposals to prospects and clients
- Develop and expand network of community contacts to maximize business development opportunities
- Cooperate with and engage support of operations staff to assure business is serviced successfully
- Meet and exceed monthly sales quotas
- Demonstrate the company core values, operating principles and service differentiators
- Document and maintain accurate information in database

TASER International Inc., Scottsdale, AZ *03/2004 – 11/2009*
National Field Services Manager

- Oversaw the scheduling and training of all support personnel
- Directed field service personnel who performed on-site routine services including installation, maintenance and repair
- Trained, motivated, counseled and monitored the performance of all customer and technical support department staff
- Managed all support personnel to ensure that customers are retained, satisfied and that their needs are fulfilled
- Managed resources to achieve service goals and assigned work schedules to ensure quality and timely delivery of service
- Instructed TASER Technicians Course to Law Enforcement and Military agencies Worldwide
- Developed new prospects and interacted with existing customers to increase sales of products and/or services

Military Experience

United States Army Reserve

First Lieutenant (P), Company Commander *03/2016 - Present*

First Lieutenant, Platoon Leader *7/2010 – 3/2016*

- Responsible for designing, executing and evaluating training exercises to ensure platoon can fulfill its mission
- Develop the management and leadership abilities of junior Non-Commissioned Officers
- Command, direct and lead military police units in both tactical and peacetime environments
- Prepare plans, policies and regulations pertaining to organization, training, operations and equipment of military police units and personnel for both combat and law enforcement operations
- Coordinated and implemented security parameters in collaboration with multiple foreign embassies, foreign militaries, governmental and non-governmental agencies located in Kabul, Afghanistan
- Liaison to base commander for a Forward Operating Base located in Kabul, Afghanistan for all base defense and force protection matters

Education

DeVry University, Phoenix, AZ **02/2004**
B.S., Network and Communications Management

U.S. Army Officer Candidate School, Fort Benning, GA **03/2011**

U.S. Army Military Police Basic Officer Leaders Course, Fort Leonard Wood, MO **08/2011**

EXPERIENCE AND QUALIFICATIONS

TASER provides body-worn cameras to Law Enforcement, and has been providing these services for 9 years. Founded in 1993, we first transformed law enforcement with our conducted electrical devices. Today, we continue to define smarter policing with our growing suite of technology solutions, including Axon body-worn video cameras and Evidence.com, secure cloud-based digital evidence management.

- As of the date of our response, TASER has 591 employees.
    - Engineering ~100
    - Manufacturing ~160
    - Sales ~125
    - Operations/Supply Chain ~25
    - Finance~20
    - Marketing ~15
    - Product Management~20
    - Customer Support ~ 20
    - Professional Services ~25
    - Legal~15
    - Administration~45
    - Quality Assurance ~25
    - Information Security ~15

- TASER's Dun and Bradstreet number is 832176382 and our Federal Tax ID is 86-0741227.

Our most experienced and skilled personnel will be involved in the implementation, development, deployment, management, and support of the FLPD's body-worn camera and digital evidence management program. Our team has the experience to evaluate the FLPD's unique situation and deploy personnel as necessary. The FLPD will have access to TASER's personnel throughout the life of the project to ensure that the FLPD's deployment is completed successfully and on time.

The amount of TASER Professional Services personnel deemed necessary once an implementation kickoff is conducted, will be available to lead the implementation, set-up, follow-up and support of your Axon and Evidence.com program within the City's timeline.

Qualifications

Through Axon and Evidence.com, TASER has deployed over 50,000 body worn camera (BWC) units and 76,000 TASER cam recorders to the Law Enforcement community:

- More than 3,500 police agencies have purchased Axon cameras in the U.S.
- More than 154,000 cameras have been purchased globally including Axon Body, Axon Flex, and TASER Cam recorders.
- 31 members of the Major City Chiefs Association have adopted TASER's Axon body cameras and evidence management suite.
- More than 5,500 police agencies use Evidence.com and have collectively stored over two Petabytes of data on Evidence.com.

With TASER, FLPD is leveraging all of the benefits of utilizing an integrated platform of technologies and cloud services. Instead of managing your own infrastructure and the unpredictable costs of scaling and managing proprietary storage arrays, Evidence.com offers continual industry best practices and services allowing **instantaneous and cost-effective scalability.**

This saves your Department from investing in and managing: storage (servers), backup storage (redundancy), staff and on-going maintenance, electrical power and cooling, space for infrastructure, networking (switches, routers, cabling, etc.). That is why there is such a movement towards implementing these solutions for managing your digital evidence.

Our ability to instantly scale its offerings to agencies of any size, along with our unparalleled implementation and post-sale support services, explain why 95% of the major U.S. agencies deploying body camera programs chose TASER's Axon cameras and evidence management suite. TASER is uniquely suited to meet the end-to-end requirements of the FLPD, today and as the agency's needs evolve.

We believe that the video evidence capture and management market will continue to expand due to several factors including increasing recognition of the benefits of video evidence. Given our existing long-term relationships with law enforcement agencies as well as our industry-leading video products, we believe we are well positioned to benefit from this growth. Our products can significantly reduce liability risk for individual police officers and for law enforcement agencies by capturing the 'truth' of what actually happened in an incident, saving law enforcement agencies significant resources.

In addition, our video products work on a stand-alone basis, or seamlessly integrated together, to automate key workflows, including the ingestion of videos recorded into our system and integration with other systems, and thus improves officer efficiency by reducing report documentation workload while increasing accuracy and accountability.

TASER and the technology we produce has a proven track record. For over 23 years, we have focused on law enforcement technology and – as the jobs of law enforcement officers evolve – so does our technology. When you partner with TASER, you join a network of agencies across the country working to improve law enforcement technology today and tomorrow.

Our hardware is reliable and designed to balance simplicity with performance. Although battery life is just one specification of a body worn camera, it is crucially important that cameras last for the officer's entire shift. Axon cameras have industry-leading battery life and are designed to last for an officer's full shift.

TASER's cost structure eliminates surprises and offers budget certainty. In this proposal, we have provided plans that are transparent and offer a fixed cost program to accommodate for the growing need for critical evidence storage.

TASER is the market leader in part because our products are backed by a team that is as dedicated to your successful deployment as you are.

Sustainable Business Practices

We take every action to minimize its impact to the environment. TASER recognizes and is fully compliant with all local, state, federal and foreign government requirements including, but not limited to, U.S. EPA and O.S.H.A. standards. TASER operates in compliance with ISO 14001, but is not currently certified.

Waste Minimization Program

TASER is committed to excellence and leadership in protection of the environment. We strive to minimize adverse impact on the air, water, and land through excellence in pollution prevention and waste abatement. By preventing pollution at the source, we save resources, increase operational efficiencies, and maintain a safe and healthy work environment for our employees, visitors, contractors, and neighbors.

The objective of TASER's Waste Minimization Program is to reduce the quantity of non-hazardous solid waste produced, recycle materials and reuse materials.

We substitute non-hazardous or less toxic material in our manufacturing processes when feasible. Examples are:

- Substituting alcohol-based glue accelerator for aliphatic petroleum-based
- Replacing the gluing system with a less hazardous two-component epoxy

TASER engages in the following practices to reduce the impact on the environment.

Use of Recycled Materials

- Use of corrugated materials that exceeds the required minimum of 35% post-consumer recycled content
- Use of other packaging materials that contain recycled content and are recyclable in most local programs
- Promotes waste prevention and source reduction by reducing the extent of the packaging and/or offering
- Packaging take-back services, or shipping carton return
- Reduces or eliminates materials which have been bleached with chlorine or chlorine derivatives

Corrugated material boxes are used that have post-consumer recycled content. Percentage is being confirmed. To minimize packaging waste on larger orders, 'bulk packaging' was created for cartridges, CEW's, and Axon products. The protective foam is recyclable once the glue is removed, and the outer boxes, both printed and corrugated are all recyclable. Chipboard boxes are from virgin materials, there's no post-consumer content in these. TASER has invested in re-usable material handling systems, much of which is also recyclable.

Environmentally Conscious Business and Manufacturing Practices

5-10% of the plastics used in manufacturing our products are made of recycled materials. TASER engages in the following practices that serve to reduce or minimize an impact to the environment, including, but not necessarily limited to,:

- Recycled materials in the warehouse and other operations
- Corrugated boxes are broken down and processed for recycling
- TASER Employee Transportation programs are in place using company supplied vans that reduce congestion on the roadways and carbon monoxide emissions into the environment

Largest Installations

Los Angeles Police Department

In 2015 TASER was awarded the contract for LAPD's deployment of 800 Axon Body Worn Cameras. This contract included technical services to assist LAPD's Tactical Technology Unit to ensure the deployment of 800 Axon Body Worn cameras without any adverse impact on the Police Department's IP networks.
Also, as part of the contract, TASER Professional Services assisted the training of the 800 officers in a manner that ensured quick turn around and use of the cameras in the field. The success of this roll-out contributed to TASER being awarded the contract for LAPD's 8,000 unit contact in 2016.

San Diego Police Department

In 2015 TASER was awarded the contract for SDPD's deployment of Axon Body Worn Cameras. This contract included technical services to assist SDPD's IT and Telecommunication teams to ensure the deployment of 1000 Axon Body Worn cameras without any adverse impact on the Police Department's or City's IP networks. Also, as part of the contract, TASER Professional Services assisted the training of the 1000 officers in a manner that ensured quick turn around and use of the cameras in the field. Deployment of the 1000 cameras was performed in three phases of 300 cameras for phase 1, 300 for phase 2, and 400 for phase 3. Each deployment phase corresponded to the deployment of three substations. Due to the success of the first phase, the second and third phases were expedited to ensure a complete roll-out.

Fort Worth Police Department

In 2013 TASER was awarded the contract for Fort Worth PD's initial deployment Axon Body Worn Cameras and Evidence.com VMS with storage. Training of the officers was conducted by TASER staff and Fort Worth's training division to ensure and optimal training experience for the officers. The success of this roll-out contributed to TASER being awarded the contract for FWPD's 400 unit contact in 2014. At this time, Fort Worth Police Department has 600+ cameras.

EXPERIENCE AND QUALIFICATIONS

TASER provides body-worn cameras to Law Enforcement, and has been providing these services for 9 years. Founded in 1993, we first transformed law enforcement with our conducted electrical devices. Today, we continue to define smarter policing with our growing suite of technology solutions, including Axon body-worn video cameras and Evidence.com, secure cloud-based digital evidence management.

- As of the date of our response, TASER has 591 employees.
    - Engineering ~100
    - Manufacturing ~160
    - Sales ~125
    - Operations/Supply Chain ~25
    - Finance~20
    - Marketing ~15
    - Product Management~20
    - Customer Support ~ 20
    - Professional Services ~25
    - Legal~15
    - Administration~45
    - Quality Assurance ~25
    - Information Security ~15

- TASER's Dun and Bradstreet number is 832176382 and our Federal Tax ID is 86-0741227.

Our most experienced and skilled personnel will be involved in the implementation, development, deployment, management, and support of the FLPD's body-worn camera and digital evidence management program. Our team has the experience to evaluate the FLPD's unique situation and deploy personnel as necessary. The FLPD will have access to TASER's personnel throughout the life of the project to ensure that the FLPD's deployment is completed successfully and on time.

The amount of TASER Professional Services personnel deemed necessary once an implementation kickoff is conducted, will be available to lead the implementation, set-up, follow-up and support of your Axon and Evidence.com program within the City's timeline.

Qualifications

Through Axon and Evidence.com, TASER has deployed over 50,000 body worn camera (BWC) units and 76,000 TASER cam recorders to the Law Enforcement community:

- More than 3,500 police agencies have purchased Axon cameras in the U.S.
- More than 154,000 cameras have been purchased globally including Axon Body, Axon Flex, and TASER Cam recorders.
- 31 members of the Major City Chiefs Association have adopted TASER's Axon body cameras and evidence management suite.
- More than 5,500 police agencies use Evidence.com and have collectively stored over two Petabytes of data on Evidence.com.

With TASER, FLPD is leveraging all of the benefits of utilizing an integrated platform of technologies and cloud services. Instead of managing your own infrastructure and the unpredictable costs of scaling and managing proprietary storage arrays, Evidence.com offers continual industry best practices and services allowing **instantaneous and cost-effective scalability.**

This saves your Department from investing in and managing: storage (servers), backup storage (redundancy), staff and on-going maintenance, electrical power and cooling, space for infrastructure, networking (switches, routers, cabling, etc.). That is why there is such a movement towards implementing these solutions for managing your digital evidence.

Our ability to instantly scale its offerings to agencies of any size, along with our unparalleled implementation and post-sale support services, explain why 95% of the major U.S. agencies deploying body camera programs chose TASER's Axon cameras and evidence management suite. TASER is uniquely suited to meet the end-to-end requirements of the FLPD, today and as the agency's needs evolve.

We believe that the video evidence capture and management market will continue to expand due to several factors including increasing recognition of the benefits of video evidence. Given our existing long-term relationships with law enforcement agencies as well as our industry-leading video products, we believe we are well positioned to benefit from this growth. Our products can significantly reduce liability risk for individual police officers and for law enforcement agencies by capturing the 'truth' of what actually happened in an incident, saving law enforcement agencies significant resources.

In addition, our video products work on a stand-alone basis, or seamlessly integrated together, to automate key workflows, including the ingestion of videos recorded into our system and integration with other systems, and thus improves officer efficiency by reducing report documentation workload while increasing accuracy and accountability.

TASER and the technology we produce has a proven track record. For over 23 years, we have focused on law enforcement technology and – as the jobs of law enforcement officers evolve – so does our technology. When you partner with TASER, you join a network of agencies across the country working to improve law enforcement technology today and tomorrow.

Our hardware is reliable and designed to balance simplicity with performance. Although battery life is just one specification of a body worn camera, it is crucially important that cameras last for the officer's entire shift. Axon cameras have industry-leading battery life and are designed to last for an officer's full shift.

TASER's cost structure eliminates surprises and offers budget certainty. In this proposal, we have provided plans that are transparent and offer a fixed cost program to accommodate for the growing need for critical evidence storage.

TASER is the market leader in part because our products are backed by a team that is as dedicated to your successful deployment as you are.

Sustainable Business Practices

We take every action to minimize its impact to the environment. TASER recognizes and is fully compliant with all local, state, federal and foreign government requirements including, but not limited to, U.S. EPA and O.S.H.A. standards. TASER operates in compliance with ISO 14001, but is not currently certified.

Waste Minimization Program

TASER is committed to excellence and leadership in protection of the environment. We strive to minimize adverse impact on the air, water, and land through excellence in pollution prevention and waste abatement. By preventing pollution at the source, we save resources, increase operational efficiencies, and maintain a safe and healthy work environment for our employees, visitors, contractors, and neighbors.

The objective of TASER's Waste Minimization Program is to reduce the quantity of non-hazardous solid waste produced, recycle materials and reuse materials.

We substitute non-hazardous or less toxic material in our manufacturing processes when feasible. Examples are:

- Substituting alcohol-based glue accelerator for aliphatic petroleum-based
- Replacing the gluing system with a less hazardous two-component epoxy

TASER engages in the following practices to reduce the impact on the environment.

Use of Recycled Materials

- Use of corrugated materials that exceeds the required minimum of 35% post-consumer recycled content
- Use of other packaging materials that contain recycled content and are recyclable in most local programs
- Promotes waste prevention and source reduction by reducing the extent of the packaging and/or offering
- Packaging take-back services, or shipping carton return
- Reduces or eliminates materials which have been bleached with chlorine or chlorine derivatives

Corrugated material boxes are used that have post-consumer recycled content. Percentage is being confirmed. To minimize packaging waste on larger orders, 'bulk packaging' was created for cartridges, CEW's, and Axon products. The protective foam is recyclable once the glue is removed, and the outer boxes, both printed and corrugated are all recyclable. Chipboard boxes are from virgin materials, there's no post-consumer content in these. TASER has invested in re-usable material handling systems, much of which is also recyclable.

Environmentally Conscious Business and Manufacturing Practices

5-10% of the plastics used in manufacturing our products are made of recycled materials. TASER engages in the following practices that serve to reduce or minimize an impact to the environment, including, but not necessarily limited to,:

- Recycled materials in the warehouse and other operations
- Corrugated boxes are broken down and processed for recycling
- TASER Employee Transportation programs are in place using company supplied vans that reduce congestion on the roadways and carbon monoxide emissions into the environment

Largest Installations

Los Angeles Police Department

In 2015 TASER was awarded the contract for LAPD's deployment of 800 Axon Body Worn Cameras. This contract included technical services to assist LAPD's Tactical Technology Unit to ensure the deployment of 800 Axon Body Worn cameras without any adverse impact on the Police Department's IP networks.
Also, as part of the contract, TASER Professional Services assisted the training of the 800 officers in a manner that ensured quick turn around and use of the cameras in the field. The success of this roll-out contributed to TASER being awarded the contract for LAPD's 8,000 unit contact in 2016.

San Diego Police Department

In 2015 TASER was awarded the contract for SDPD's deployment of Axon Body Worn Cameras. This contract included technical services to assist SDPD's IT and Telecommunication teams to ensure the deployment of 1000 Axon Body Worn cameras without any adverse impact on the Police Department's or City's IP networks. Also, as part of the contract, TASER Professional Services assisted the training of the 1000 officers in a manner that ensured quick turn around and use of the cameras in the field. Deployment of the 1000 cameras was performed in three phases of 300 cameras for phase 1, 300 for phase 2, and 400 for phase 3. Each deployment phase corresponded to the deployment of three substations. Due to the success of the first phase, the second and third phases were expedited to ensure a complete roll-out.

Fort Worth Police Department

In 2013 TASER was awarded the contract for Fort Worth PD's initial deployment Axon Body Worn Cameras and Evidence.com VMS with storage. Training of the officers was conducted by TASER staff and Fort Worth's training division to ensure and optimal training experience for the officers. The success of this roll-out contributed to TASER being awarded the contract for FWPD's 400 unit contact in 2014. At this time, Fort Worth Police Department has 600+ cameras.

APPROACH TO SCOPE OF WORK

Operational Plan

TASER will assist in implementing FLPD's body-worn camera program in the following ways.

Leadership

TASER will provide FLPD with a team of experienced professionals to ensure an efficient deployment of Axon body cameras. Your team will consist of:

- Project Manager to oversee all events leading to body camera deployment completion
- Systems Engineer to oversee all network/technical needs and integrations with your current systems (e.g. CAD/RMS integration, Axon Signal activation, etc.)
- Account Manager to provide support with camera and Axon Dock, equipment setup and post-production needs related to technical support
- Professional Service Manager to assist with officer and administrative training

The team will work closely with FLPD's Project Manager to align resources and accomplish the tasks necessary for an efficient deployment and training process.

Coordination

If requested, TASER will align user trainings with officers' shift schedules, in order to minimize disruption in FLPD's daily functions. Other tasks, including equipment configurations, consultative implementation services, and administrative trainings, will be scheduled around FLPD's preferences as well.

Implementation

TASER's Professional Services team will provide the following services for Axon camera deployment:

System Set Up and Configuration

- Setup Axon View on smart phones (if applicable).
- Configure categories & custom roles based on Agency need.
- Troubleshoot IT issues with Evidence.com and Axon Dock access.
- Work with IT to install Evidence Sync software on locked-down computers (if applicable).

Axon Dock Installation

- Work with Agency to decide ideal location of Axon Dock setup and set configurations on Axon Dock if necessary.
- Authenticate Axon Dock with Evidence.com using “admin” credentials from Agency.
- Work with Agency’s IT to configure its network to allow for maximum bandwidth and proper operation within Agency’s network environment.

Best Practices for Implementation Planning

- Provide considerations for establishment of video policy and system operations best practices based on TASER’s observations with other agencies.
- Discuss importance of entering meta-data in the field for organization purposes and other best practice for digital data management.
- Provide referrals to other agencies using the Axon camera products and Evidence.com services.
- Recommend roll out plan based on review of shift schedule

System Administrator and Troubleshooting Training Sessions

- Provide a step-by-step explanation and assistance for Agency’s configuration of security, roles & permissions, categories & retention, and other specific settings for Evidence.com.

Axon /Instructor Training

- Prior to general user training on Axon camera systems and Evidence.com services, TASER’s on-site professional services team will provide training with the goal of certifying instructors who can support the Agency’s subsequent Axon camera and Evidence.com training needs.

End User Go-Live Training and Support Sessions

- Provide individual device set up and configuration assistance; pairing with viewers when applicable; and training on device use, Evidence.com and Evidence Sync.

Implementation Document Packet

- Evidence.com administrator guides, camera implementation guides, network setup guide, sample policies, and categories & roles guide.

Integration with CAD/RMS

- TASER will develop an integration module that allows the Evidence.com services to interact with the Agency's CAD/RMS so that Agency's licensees may use the integration module to automatically tag the Axon recorded videos with a case ID, category, and location. The integration module will allow the Integration Module License holders to auto populate the Axon video meta-data saved to the Evidence.com services based on data already maintained in the Agency's RMS.

Project Manager/Reporting

- TASER will assign a dedicated Project Manager to work with FLPD on all aspects of planning the Axon body-worn camera roll out. Prior to roll out, the Project Manager will develop a Project Plan and Checklist for the deployment of Axon camera units, Axon Docks and Evidence.com account training. He/she will also work closely with FLPD's Project Manager to ensure that all integrations, configurations and trainings are completed or scheduled prior to deployment.

Support and Maintenance

- TASER has a full Customer Support division. Customer Service is available 24/7 via email, and live phone support Monday-Friday, 7:00AM – 5:00PM MST. For technical or Customer Service assistance, please contact 800-978-2737 or customerservice@taser.com. TASER also has a dedicated line available for emergencies, with a live Support Specialist available 24/7.

  In addition to TASER's Customer Service team, an experienced Account Manager will be assigned to your Agency. He/she will work closely with your leadership team and provide maintenance and technical support before and after deployment.

Methodology

TASER's Project Management Methodology (PMM) provides a series of roadmaps for personnel to navigate toward a common set of goals. The PMM provides the project tracking, risk, problem, communication, quality, and change management processes and tools that are key to successful management of information technology projects. During the implementation kick-off, the TASER Project Manager will tailor the methodology to align with the specific objectives and requirements of the FLPD. The resulting concepts, tools, and techniques will be shared with each member of the team and will become a way of life for the project staff. This will provide the structure, focus, and discipline needed to successfully deliver a project of this size and complexity.

The key to PMM is its use of continuous quality management, which includes two levels of quality assurance throughout the project. First is the quality assurance of project deliverables. Our Project Manager will be responsible for verifying that each project deliverable meets the requirements of the contract and that the appropriate reviews/inspections are performed by the FLPD. Most importantly, our Project Manager will confirm that any issues are addressed in a timely and appropriate manner. The second level of quality assurance is periodic project reviews. These reviews measure compliance to sound Project Management practices as defined by the PMM. For this project, we will be responsible for managing our staff resources assigned to the project and for coordinating with the FLPD Project Manager, who will coordinate activities according to the mutually agreed to project plan.

Our project team is experienced in managing all aspects of large-scale implementations. Our extensive experience allows us to anticipate potential risks and to take corrective actions early so that project scope, schedule, and budget are not impacted.

We have four basic objectives in managing a project, which are the foundation of any sound project management methodology:

- High-quality work: Deliver high quality end products, address business objectives, and meet end user requirements.
- On-time delivery: Complete deliverables on schedule and within budget.

- Effective Communication: Maintain timely and accurate communication to project participants throughout the entire project.
- Aggressive management: Identify potential problems before they develop, and initiate appropriate corrective action

Sample Statement of Work

The following Statement of Work has been used during the successful of a number of large agencies including the Los Angeles Police Department and San Antonio Police Department.

1. Sample Statement of Work

STATEMENT OF WORK FOR THE IMPLEMENTATION OF THE FT. LAUDERDALE POLICE DEPARTMENT'S AXON BODY-WORN CAMERA AND EVIDENCE.COM PROGRAM

Submitted by:

TASER International, Inc.

17800 North 85th Street
Scottsdale, AZ 85255
800.978.2737

TABLE OF CONTENTS

1. PROJECT SUMMARY

This Statement of Work outlines the responsibilities of TASER and the FLPD for implementing the rollout of Axon Body-Worn Cameras and Evidence.com within FLPD's organization.

1.1 Project Scope.

The Axon Camera and Evidence.com deployment will be completed over four phases within one year, October 2015 – September 2016. TASER will provide the following deliverables to help effectively deploy TASER Services and Products within the timeline set forth by FLPD:

- Evidence.com account set up
- Axon Mobile app installation
- Roles/Permissions set-up assistance
- Delivery of Axon hardware
- Evidence Dock configuration assistance
- Assistance with set up of Evidence.com user accounts
- Training
- Integration with CAD/RMS System

1.2 Out of Scope Services.

TASER is responsible to perform only the Services described above in Section 1.1. Any additional services discussed or implied that are not defined explicitly by this SOW will be considered out of the scope. This project scope does not include the administration, management, or support of any internal City IT network or infrastructure.

2. PROJECT MANAGEMENT.

TASER will assign a Project Manager that will provide the expertise to execute a successful body camera deployment and implementation. The Project Manager will have significant knowledge and experience with all phases of the project management lifecycle and with all application modules being implemented. He/she will work closely with FLPD's Project Manager and project team members and will be responsible for completing the tasks required to meet all contract deliverables on time and on budget.

2.1 Project Management Reporting, Documentation and Communication Strategy.

The attached Project Plan includes a comprehensive project plan outlining the tasks, responsibilities and schedule for the first phase of FLPD's body camera roll-out.

After obtaining agreement from FLPD on the project plan and rollout schedule, TASER's Project manager will ensure all team members from TASER and FLPD are continually updated on the status of the body camera program through:

- Development of a communication plan for implementation
- Weekly status meetings via conference call/webinar
- Project briefings to **FLPD**'s Management team as requested
- Configuration manuals and best practices documentation

3. PROFESSIONAL SERVICES.

TASER's professional services team consists of Customer Support Specialists, Sales Engineers, Trainers and Project Managers to help with all phases of FLPD's deployment.

3.1. Pre-Deployment Assistance.

Prior to the go-live date for each phase of the deployment, TASER's Professional Services team will perform the following tasks:

- **Evidence.com account set up:** TASER will send an Evidence.com invite email to FLPD's designated administrator. The administrator must accept the Invitation to initiate access to Evidence.com. This task is completed prior to the initial launch of project but not for subsequent phases.

- **Axon Mobile app:** TASER will pre-download the Axon Mobile app on devices purchased through TASER. If using the app on personal or department-assigned devices, installation of the free app will be supported during training through the Apple/Android App stores.

- **Roles/Permissions set-up assistance:** TASER can provide a step-by-step explanation and assistance for FLPD's configuration of categories, custom roles and permissions within the Evidence.com Admin tab.

- **Delivery of Axon hardware:** TASER will send all equipment per contract requirements via FedEx and provide tracking information to FLPD.
- **Evidence Dock configuration:** Taser will provide 2 days of on-site assistance for configuring Evidence Docks (see manual for specific instructions: *https://www.taser.com/images/support/downloads/downloads/Evidence_com_Dock_Installation_Guide.pdf*). TASER can assist with dock configuration if requested.

3.2. Training.

TASER will provide one week of on-site training to lead the first phase of the Axon deployment. The trainings include:

End-user go-live training and support: This training provides individual device set up and configuration assistance, pairing with viewers when applicable, and training on device use, Evidence.com and Evidence Sync. The training also includes policy overview by the agency leadership team. (average training time: 3 hours).

Administrator training: This training provides a deep dive into Evidence.com for staff members that will be using Evidence.com but not wearing a camera. It covers topics such as building cases, searching users and sharing data within and outside of the Agency. The training can be customized to the needs of the individual Agency (average training time: 2 hours).

Axon Instructor training: This training provides instruction to FLPD in-house trainers, with the goal of certifying instructors who can support FLPD's subsequent Axon camera and Evidence.com training needs (average training time: 4 hours).

3.3. Support and Maintenance.

TASER has a full Customer Support division. Customer Service is available 24/7 via email and live phone support Monday-Friday, 7:00AM – 5:00PM MST. For technical or Customer Service assistance, FLPD can contact 800-978-2737 or customerservice@taser.com. TASER also has a dedicated line available for emergencies, with a live Support Specialist available 24/7.

In addition to TASER's Customer Service team, an experienced Support Manager will be assigned to FLPD. He/she will cover post-production needs related to maintenance and technical support on all hardware and software.

3.4. CAD/RMS integration.

The CAD/RMS integration will consist of the development of an integration module that allows the Evidence.com services to interact with the FLPD's CAD/RMS. Licensees may use the integration module to automatically tag the Axon recorded videos with data already maintained in the Agency's CAD/RMS, including, but not limited to, a case ID, category, and location.

Projected completion of the integration is **<<date>>**. After completion acceptance by FLPD, TASER will provide up to 5 hours of remote (phone or Web-based) support services at no additional charge to the Agency. TASER will also provide support services that result because of a change or modification in the Evidence.com services at no additional charge as long as FLPD maintains Evidence.com subscription licenses and Integration Module Licenses, and as long as the change is not required because FLPD changes its RMS. Thereafter, any additional support services provided to FLPD will be charged at TASER's then current standard professional services rate.

3.5 Acceptance Checklist.

TASER will present FLPD with an Acceptance Checklist (Checklist) upon TASER's completion of the Services and Integrations. FLPD will sign the Checklist acknowledging completion of the Services and Integrations once the on-site service session has been completed.

If FLPD reasonably believes that TASER did not complete the Services and Integrations in substantial conformance with this SOW, FLPD will notify TASER in writing of its specific reasons for rejection of the Services within 14 calendar days from delivery of the Checklist to FLPD. TASER will address FLPD's issues and then will re-present the Checklist for approval and signature.

3.6 Key Assumptions.

The Services, fees, and delivery schedule for this project are based on the following assumptions:

A. Agency's relevant systems are available for assessment purposes prior to TASER's arrival at the Installation Site.
B. All work will be performed by TASER's personnel during normal business hours, Monday through Friday, 8:30 a.m. to 5:30 p.m., except holidays unless otherwise agreed to in advance.
C. All tasks on-site will be performed over a consecutive timeframe unless otherwise agreed to by TASER and Agency.

D. Agency representatives will be available to provide timely and accurate information.

4. FLPD RESPONSIBILITIES

In order to fulfill the deliverables listed in this SOW, FLPD is responsible for contributing to project status reports, reporting project issues, and providing internal resources to assist with hardware and software set-up and configuration.

4.1 FLPD Tasks.

To ensure a successful deployment, FLPD will be responsible for completing the following pre-deployment configuration tasks:

- **Set up Evidence.com user accounts:** Within the Evidence.com Admin tab, FLPD can upload users to Evidence.com and invite users via email to sign into their individual accounts: *http://public.evidence.com/help/pdfs/ latest/Evidence.com+Administrator+ Reference+Guide.pdf, pg. 18.*

- **Create video policy**: Before camera deployment, FLPD should define the agency video policy and create categories and evidence retention levels for videos. FLPD should also establish method for officers to add metadata to videos (e.g. Axon Mobile, CAD integration, Evidence.com).

- **Evidence Dock installation:** Determine ideal location of Dock setup, install docks, and set configurations on Docks (see manual for specific instructions: *https://www.taser.com/images/support/downloads/downloads/Evidence_com_Dock_Installation_Guide.pdf*). TASER can assist with dock configuration if requested.

- **Download Evidence Sync**: Install Evidence Sync software on computers in the Report Writing Room(s) and on MDTs (*https://TASER.taser.com/info/sync-registration.* TASER can also provide an enterprise-deployable version of SYNC.

- **Troubleshooting reporting:** Agency will alert TASER of any IT issues with Evidence.com or Dock access so TASER can remedy before live deployment.

4.2. Expectations.

TASER's successful performance of the Services depends upon your:

A. Making available its relevant systems, including its current RMS, for assessment by TASER (including making these systems available to TASER via remote access if possible);
B. Making any required modifications, upgrades or alterations to your hardware, facilities, systems and networks related to TASER's performance of the Services prior to TASER's arrival at the Instillation Site;
C. Providing access to the building facilities and where we are to perform the Services, subject to safety and security restrictions imposed by you (including providing security passes or other necessary documentation to our representatives performing the Services permitting them to enter and exit your premises with laptop personal computers and any other materials needed to perform the services);
D. Providing all necessary infrastructure information (TCP/IP addresses, node names and network configuration) necessary for us to provide the Services;
E. Promptly installing and implementing any and all software updates provided by TASER;
F. Ensuring that all appropriate data backups are performed;
G. Providing TASER with remote access to its Evidence.com account when required for TASER to perform the Services;
H. Identifying in advance any holidays, non-work days, or major events that may impact the project;
I. Making any required modifications, upgrades or alterations to Agency's hardware, facilities, systems and networks related to TASER's performance of the Integration Services;
J. Providing to TASER the assistance, participation, review and approvals and participating in testing of the Integration Services as requested by TASER;
K. Notifying TASER of any network or machine maintenance that may impact the performance of the integration module at the Agency;
L. Ensuring the reasonable availability by phone or email of knowledgeable staff and personnel, system administrators, and operators to provide timely, accurate, complete, and up-to-date documentation and information to TASER (these contacts are to provide background information and clarification of information required to perform the Integration Services).

5. CHANGES TO SERVICES

Changes to the services set forth in this SOW must be documented and agreed upon by the parties in a change order. If the changes cause an increase or decrease in any charges or cause a scheduling change from that originally agreed upon, an equitable adjustment in the charges or schedule will be agreed upon by the parties and included in the change order, signed by both parties.

Training Plan

TASER can help the FLPD maximize your Axon and Evidence.com investment with comprehensive implementation and custom integration services (if applicable). The TASER Professional Services team consists of a group of highly skilled individuals with in-depth knowledge of all TASER, Axon and Evidence.com products. The full-service professional services package includes a dedicated Project Manager who will create a custom project plan to fit the FLPD's needs. On-site system configuration and setup along with on-site go-live training and support is also included.

Additional packages and services are available, including CAD/RMS Integrations and Network or Application Security Assessments, custom-designed to analyze FLPD's information security posture.

There are other benefits with TASER Professional Services, such as subject matter experts who consult on best practices for setup, configuration, policy and overall program performance. Agency program success is three times greater where Professional Services has rendered on-site support, than where we have not.

Our Professional Services Managers focus entirely on on-site and off-site training. Our experienced team can train everyone from officers, administrators, armorers, supervisors, detectives and even prosecutors.

TASER recommends a train-the-trainer model, which tends to work well for our Law Enforcement customers. This model will enable the FLPD to train officers based on their schedules and availability. As more Axon cameras are added to the Agency, those trainers can provide the same level of training at no additional cost.

Install, Configure and Test Your System

During this phase of implementation, TASER's Professional Services team will assist with the following tasks:

1. System Set Up and Configuration

- Setup Axon View on smart phones (if applicable).
- Configure categories & custom roles based on Agency need.
- Troubleshoot IT issues with Evidence.com and Axon Dock access.
- Work with IT to install Evidence Sync software on locked-down computers (if applicable).

2. Axon Dock Installation

- Work with Agency to decide ideal location of Axon Dock setup and set configurations on Axon Dock if necessary.
- Authenticate Axon Dock with Evidence.com using “admin” credentials from Agency.
- Work with Agency’s IT to configure its network to allow for maximum bandwidth and proper operation within Agency’s network environment.

3. Train the First Wave

An initial, limited number of Key Users, Armorer(s) and System Administrator(s) should be trained. The size of this contingent depends on agency size or size of the planned full deployment. These officers will serve a number of roles, including final confirmation of system functionality and performance. They will likely provide useful feedback on any localized issues that had not been previously identified. They will provide a demonstration and information platform for their co-worker/future User Officers. They typically become a resource when newer Users are activated and require training or assistance.

For every agency on Evidence.com, a ‘Super Administrator’ account is created by TASER during the initial implementation cycle. Typically, the ‘Super Administrator’ is the individual most responsible for the agency’s Evidence.com account.

This will be the first user account and the starting point for defining security settings, creating custom roles and setting permissions, adding users (User, Administrator, Armorer or any other custom roles), reassigning devices, creating categories and setting retention policies, and several of the other administrative features of the Evidence.com services. This account does not differ from other Administrator accounts setup within the agency. It is called Super Administrator only because it is the first account that is required to be set up for a new agency.

Our team will provide step-by-step explanations and assistance for Agency’s configuration of security, roles & permissions, categories & retention, and other specific settings for Evidence.com. Administrators should attend all of the training sessions that are decided upon.

TASER will then provide Axon Instructor training with the goal of certifying instructors who can support the Agency's subsequent training needs. We recommend a train-the-trainer model for Law Enforcement customers, as it enables FLPD to train new officers based on their schedules and availability. As more Axon cameras are added to the Agency, those trainers can provide the same level of training at no additional cost to the Agency.

Axon recordings can be used to enhance new-officer or in-service training. Many training academies and Field Training Programs have improved upon the quality of training provided and reduced the time required waiting for opportunities to encounter certain high-risk/low-frequency events.

4. Start Small, Test, Assess, Correct, and then Go Big

Deploy the Key Users. Make sure the way you've configured your system integrates smoothly into your workflow. Assess readiness based on evaluation and feedback and make any necessary adjustments. Once you've taken these steps, you're ready to schedule the rest of your User training.

5. End-User Training

During on-site training, our Professional Services team will provide the FLPD with documentation including but not limited to the following. All of these items are the FLPD's to keep for reference and use in future training sessions.

- Axon Dock Manuals
- Evidence Sync Set Up and User Manuals
- Axon Camera Quick Start Guides and User Manuals
- Evidence.com Administrator Reference Guide
- Evidence.com Security Guide
- End-to-End Deployment Guide
- Implementation Best Practices Guide and
- Go Live Checklist.

Sample Lesson Plans are included on the following pages.

AXON

Lesson Plans & Course Outlines
Train-the-Trainer

Release Date: February 2016
Version 1.0

Axon and Evidence.com

Target Audience

Trainers of the Axon body-worn camera and Evidence.com systems

Course Summary

This training provides a deep-dive into EVIDENCE.com for staff members that will be using EVIDENCE.com and teaching others how to operate the devices and software solutions. Topics include:

- Agency policy guidelines *(agency-specific)*
- Operation and fitting of the camera
- Axon Mobile app *(if applicable)*
- Evidence Sync *(if applicable)*
- Evidence.com
    - Searching Users and conducting User Audits
    - Creating reports
    - User Groups
    - Building Cases
    - Sharing data within and outside of the agency

Course Materials

- Projector
- Pre-assigned cameras
- Camera Accessories/Mounts

Pre-Training Checklist

□ Officers are invited via email to Evidence.com.
□ Officers accept invite and log into Evidence.com.
□ Cameras are assigned to all officers attending training.
□ All Axon Docks are installed and configured.
□ Body worn camera policy is completed and published.

Training Outline

1. **Policy and Project Overview (30 min – 1 hr)**

2. **Camera/Battery Overview (15 min)**
   a. Operation
   b. Specs

3. **Hands-on Demo with participants (20 min)**
   a. Turning on camera
   b. Recording sample video
   c. Ending a recording
   d. Demoing mounting options

4. **Docking Station (10 min)**
   a. Docking a camera properly
   b. Functions of dock
   c. Removing camera from dock

5. **Axon Mobile Applications – Axon View and Axon Capture (15 min)**
   a. Pairing camera to mobile device via Bluetooth
   b. Reviewing live video streaming
   c. Adding metadata to sample video

6. **Evidence Sync (20 min)**
   a. Signing into Evidence Sync
   b. Connecting camera and adding metadata
   c. Uploading evidence

7. **Overview of Evidence.com (1 – 1.5 hours)**
   a. Home page overview
   b. Evidence search
   c. User Search
   d. User Audit
   e. Managing users/devices

Training Outline *continued*

8. **Viewing Videos (15-20 mins)**
    a. Media player page overview
    b. Clips/markers
    c. Redaction
    d. Evidence audit trail

9. **Cases (15-20 mins)**
    a. Creating case
    b. Adding evidence to a case
    c. Viewing case audit trail

10. **Sharing within and outside of agency (20-30 mins)**
    a. Sharing cases
    b. Sharing individual videos

11. **Evidence management (20-30 mins)**
    a. Category retention/reassignment
    b. Reassigning ownership of videos
    c. Downloading evidence
    d. Deleting evidence

12. **User management (20-30 mins)**
    a. User search
    b. Adding/deactivating users
    c. Auditing users
    d. Creating/managing reports

13. **Device Management (20-30 mins)**
    a. Searching for a device in Evidence.com
    b. Reassigning devices
    c. RMA process for devices

AXON

Lesson Plans & Course Outlines User Training

Release Date: February 2016

Version 1.0

Axon and Evidence.com

Target Audience

End-users of the Axon body-worn camera and Evidence.com systems

Course Summary

This training course provides an overview of the Axon Body Camera and Evidence.com systems. Topics include:

- Agency policy guidelines *(agency-specific)*
- Operation and fitting of the camera
- Evidence.com
- Axon Mobile app *(if applicable)*
- Evidence Sync *(if applicable)*

Course Materials

- Projector
- Pre-assigned cameras
- Camera Accessories/Mounts

Pre-Training Checklist

□ Officers are invited via email to Evidence.com.
□ Officers accept invite and log into Evidence.com.
□ Cameras are assigned to all officers attending training.
□ All Axon Docks are installed and configured.
□ Body worn camera policy is completed and published.

Training Outline

1. **Policy and Project Overview (30 min – 1 hr)**

2. **Camera/Battery Overview (15 min)**
   a. Operation
   b. Specs

3. **Hands-on Demo with participants (20 min)**
   a. Turning on camera
   b. Recording sample video
   c. Ending a recording
   d. Demoing mounting options

4. **Docking Station (10 min)**
   a. Docking a camera properly
   b. Functions of dock
   c. Removing camera from dock

5. **Axon Mobile Applications – Axon View and Axon Capture (15 min)**
   a. Pairing camera to mobile device via Bluetooth
   b. Reviewing live video streaming
   c. Adding metadata to sample video

6. **Evidence Sync (20 min)**
   a. Signing into Evidence Sync
   b. Connecting camera and adding metadata
   c. Uploading evidence

7. **Overview of Evidence.com (40 min)**
   a. Signing in to Evidence.com
   b. Searching for evidence
   c. Viewing a video
   d. Adding metadata through Evidence.com
   e. Adding markers, clips, notes etc.
   f. Redaction (if applicable)
   g. Viewing audit trails
   h. Building cases (if applicable)

Project Plan

The implementation process begins with an on-site kickoff meeting. A Project Schedule will be created to outline the estimated timeline (including number of days necessary for each phase of the FLPD's implementation) and training specific to your program. Installations, registrations, configurations, set up of user accounts, assignment of roles and permissions, etc., will occur prior to user training sessions.

The FLPD should designate a Project Manager and an IT point of contact at your agency will be overseeing the project to facilitate communication with TASER during implementation. The FLPDwill also need to assign a staff member as the Evidence.com 'Super Administrator' – this role is created by TASER during the initial implementation cycle. This account does not differ from other Administrator accounts setup within the agency. It is called Super Administrator only because it is the first account that is required to be set up for a new agency.

Typically the 'Super Administrator' is the individual foremost responsible for the agency's Evidence.com account. The Super Administrator will be the first user account created and will serve as the starting point for Evidence.com configuration including:

- Defining security settings
- Creating custom roles and setting permissions,
- Adding users (User, Administrator, Armorer or any other custom roles)
- Assigning and reassigning devices
- Creating categories and setting retention policies, and;
- Several of the other administrative features of the Evidence.com services.

TASER will provide the FLPD with a team of experienced professionals to ensure an efficient deployment of Axon Body cameras.

The TASER Project Team will consist of:

- A Project Manager
  The Project Manager will develop a Project Schedule and Go Live Checklist for the deployment of Axon camera units, Axon Docks and Evidence.com account training. He/she will also work closely with FLPD's Project Manager to ensure that all integrations, configurations and trainings are completed or scheduled prior to deployment.

- A Professional Services Manager
  Your Professional Services Manager will assist with all aspects of training. If requested, TASER will align user trainings with officers' shift schedules, in order to minimize disruption in FLPD's daily functions. Other tasks, including equipment configurations, consultative implementation services, and administrative trainings, will be scheduled around FLPD's preferences as well.

- A Pre-Sales System Engineer
  Your Pre-Sales System Engineer will oversee all network/technical needs and integrations with your current systems (e.g. CAD/RMS integration, light bar activation, etc.). He will work in collaboration with the FLPD's IT point of contact to assess current bandwidth, calculate the potential network impact of the body-worn camera system and develop ways to reduce network impact. The assigned Pre-Sales System Engineer will also assist with calculating the exact network impact and development.

- A Regional Support Manager
  Your Regional Support Manager is a supplemental point of contact within TASER headquarters. Their job is to ensure a good standing health for your agency's Axon and Evidence.com program by utilizing consistent communication, virtual support, and providing the necessary resources needed to make sure you are set up for success.

FLPD Responsibilities for Planning Prior to Implementation

Based on our experience, the success of an Agency's implementation is contingent upon completing the following tasks and/or assisting TASER in the following ways.

- Provide IT and Project Manager POCs to TASER International personnel
- Making relevant systems available for assessment by TASER prior to arrival at the Instillation Site
- Making any required modifications, upgrades or alterations to hardware, facilities, systems and networks related to TASER's performance of the Services prior to TASER's arrival at the Instillation Site
- Providing access to the building facilities and where TASER is to perform the Services, subject to safety and security restrictions imposed by an agency (including providing security passes or other necessary documentation to TASER representatives performing the services, permitting them to enter and exit the premises with personal laptop computers and any other materials needed to perform the services)
- Conduct an internet bandwidth test
- Providing all necessary infrastructure information (TCP/IP addresses, node names and network configuration) necessary for TASER to provide the services
- Promptly installing any and all software updates provided by TASER
- Providing TASER with remote access to the agency's Evidence.com account when required for TASER to perform the Services
- Identifying in advance any holidays, non-work days, or major events that may impact the project
  - Define categories and evidence retention levels
  - Define roles and permissions
  - **Draft the on-officer camera video policy** - Departments that do not yet have a policy governing on-officer video systems should start drafting a policy to facilitate the implementation process. It is strongly encouraged that your department has at least a draft of your video policy completed before user training begins. This allows training to simultaneously cover both how the hardware works in conjunction with how users are expected to utilize the system.
  - Draft the officer training schedule

Communications Planning/Execution

The FLPD should designate a Project Manager and an IT point of contact in charge of overseeing the project to facilitate communication with TASER during implementation. Any member of the FLPD can communicate directly with the assigned Project Manager, Professional Services Manager, Pre-Sales Engineer and Regional Support Manager.

After obtaining agreement from the FLPD on the project plan and rollout schedule, your Project manager will ensure all TASER team members and FLPD staff are continually updated on the status of the process. The reporting, documentation and communication strategy includes the following:

- Development of a communication plan for implementation
- Weekly status meetings via conference call/webinar
- Project briefings to **FLPD**’s Management team as requested
- Configuration manuals and best practices documentation

System, Performance and User Acceptance Testing

We will present you with an Acceptance Checklist upon our completion of the Services that will exactly mirror the description of services within this Section. You will sign the Checklist acknowledging completion of the Services once the on-site service session has been completed. If you reasonably believe that we did not complete the Services in substantial conformance with this Agreement, you must notify us in writing of your specific reasons for rejection of the Services within seven calendar days from delivery of the Checklist to you. We will address your issues and then will re-present the Checklist for your approval and signature.

TASER’s Acceptance Test Plan includes the following:

- Video capture tests
- Video download tests
- Video recall tests
- Defined process for the correction of errors, defects, and deficiencies

After the Acceptance Test Plan has been reviewed and evaluated by the FLPD, TASER’s certified trainers will assist with the Acceptance Test at FLPD’s facilities in accordance with the Acceptance Test Plan.

The Acceptance Test can be scheduled at FLPD's convenience. TASER understands that the Acceptance Test will be "accepted" in writing by FLPD only when all tests are performed without error.

Final Acceptance

TASER understands that final acceptance and final payment will only be "accepted" when all tests in the Acceptance Test Plan are performed without error and the system has been used operationally and error free for 30 days, and system users are fully trained. TASER will assist FLPD in completing the Acceptance Test and will provide training to system users as outlined in this proposal.

Problem Resolution during Acceptance Testing

TASER will assist FLPD with problem resolution during acceptance testing by correcting any defects, errors, or deficiencies found in the system prior to the expiration of the warranty period. Problem resolution during the acceptance testing will be provided by TASER at no additional cost.

A sample Acceptance Test Plan is on the following pages.

USER ACCEPTANCE TESTING

1. **Introduction:** This User Acceptance Testing (UAT) document outlines the approval process for the deployment and implementation of Axon Body Cameras and Evidence.com within (Agency Name). The test criteria outlined below ensures that the Axon system satisfies the needs of the Agency as specified in the Master Service Agreement and provides confidence in its use.

2. **Test Methodology:** UAT will be conducted by end users, subject matter experts, and/or the Agency's body camera project team. Users will execute all test procedures referenced in section 3. Users may also perform additional tests not detailed in the plan but remain relevant and within the scope of the project, as mutually agreed upon by TASER and the Agency. Such additional test procedures (if any) will be attached to this document as an Appendix.

3. **UAT Plan**: This plan contains a detailed procedure of each test to be performed by the UAT team.

Axon Camera UAT Plan

Execution Procedure	Delivery	Pass/Fail
User slides camera power switch to "on" position.	Solid red LED light on Axon Body camera or Axon Flex battery pack will change to blinking green within 20 seconds. The device is now in "buffering" mode.	
User adjusts volume tone by firmly pressing diamond volume/pairing button.	Camera will cycle through 3 audible tones (low, medium, high) and mute.	
User starts recording by double-tapping event button.	Blinking green LED light on Axon Body camera or Axon Flex battery pack will change to blinking red and the camera will beep twice (provided volume is on). The camera is now in "record" mode.	
User ends recording by pressing and holding event button for 5 seconds.	Blinking red LED light on Axon Body camera or Axon Flex battery pack will change to blinking green and the camera will beep once (provided volume is on). The device is now in "buffer" mode.	
User slides power button to "off" position. While holding and pressing the pairing/volume button, user slides power button back to "on" position.	Camera will beep twice (provided volume is on) LED light on Axon Body camera or Axon Flex battery pack will start blinking. This indicates that the camera is ready to pair with a Bluetooth connected iOS or Android device.	
User selects correct device under Bluetooth settings on iOS or Android device.	iOS or Android device will indicate that the selected camera is now "connected."	

User opens Axon Mobile app on iOS or Android device.	Live stream of camera footage appears on mobile device.	
User powers down camera.	LED light on Axon Body camera or Axon Flex battery pack will display a solid red light and will shut off within 20 seconds.	
User places camera into Evidence Dock.	Within 1 minute, the camera’s LED light will either display solid yellow (queued to upload) or blinking yellow (actively uploading).	
User retrieves camera from dock before the start of his/her next shift.	Camera’s LED light changes from yellow/blinking yellow to green within 24 hours.	
Once the camera in the dock is displaying a solid green light, the user will log into Evidence.com using his/her proper credentials.	User will see a hyperlink to his/her recently uploaded videos on the homepage.	
User clicks on recently uploaded video.	User is able to play video within Evidence.com’s media player.	

Evidence.com UAT Plan

Function	**Delivery**	**Pass/Fail**
Roles and Permissions: Configurable by Agency administration.	Out of box	
Case Management Tools: Users are able to create and share cases in accordance with the permissions granted by administration.	Out of box	
Chain of Custody: An audit trail is generated for every video	Out of box	
Download videos/cases: Standard feature, granted the user has permission.	Out of box	
Reassign Evidence: Administrator may reassign evidence to another user if needed.	Out of box	
Search Functionality: Available by user name, event or device	Out of box	
Evidence Deletion: Available by permission only, with a 7-day grace period.	Out of box	
Ability to create clips/markers: Standard function available by permission.	Out of box	
Redaction: Function available on PRO licenses and with proper permission set by Agency.	Out of box	

User audit and Agency activity tracking: Function available on PRO licenses and with proper permission set by Agency.	Out of box	
Uploading: User may upload pictures, videos and digital files, regardless of recording device.	Out of box	
Track and assign all devices within Evidence.com.	Out of box	
Allows viewing and downloading of all evidence stored in Evidence.com.	Out of box	
Retention: Ability to retention level, depending on category of evidence.	Out of box	

4. **UAT Defects:** The Agency will present defect findings directly to TASER's Project Manager within seven (7) days of discovery. TASER's Project Manger will record and report the defect to the appropriate team at TASER. Each defect submitted by the UAT team will be addressed, resolved, and re-tested by the UAT team prior to closure.

5. **Signatures:**

Role	**Name**	**Signature**	**Date**
Agency Authorized Representative			
TASER Project Manager			
Other(s) (if necessary)			

Training and Documentation

Prior to implementation, TASER will make available to the FLPD the following materials in an electronic format. Training guides, user manuals and product documentation include but are not limited to the following. Documentation is separated into folders by topic. All materials are the FLPD's to access and use for future training or as needed.

- Best Practices Guide
- End-to-End Deployment Guide
- User and Administrator Training Lesson Plans
- Training Outlines
- Hardware Installation Guides
- Sample Body-Worn Camera Policies

Sample Policies and On-Officer Program Information Folder

This folder contains PDF documentation intended for Agency Head/Program Administrator roles.

- Implementation Best Practices
- Sample Policies Agency References
- Sample Policies of 20+ Agencies

Deployment Folder

This folder contains various formats of documentation intended for Agency Head/Program Administrator roles.

2016 Checklists – Pre-Deployment & Go Live Folder

- Axon BWC Go Live Checklist 2016
- Axon Deployment Glossary 2016
- Axon PS Pre Arrival Checklist 2016

API Folder

- Evidence Partner API Overview 2016 Document

Evidence Sync Guide Folder

This folder contains PDF documentation intended for Agency Head/Program Administrator roles.

- Categories Retention Schedule
- Evidence Sync User Manual (English)

Guides and Manuals Folder

This folder contains various formats of documentation intended for Agency Head/Program Administrator roles as well as end-users.

Axon Body 2

- Axon Body 2 Manual
- Axon Body 2 Videos
- Axon Body 2 Quick Start
- Axon Body 2 Spec
- Axon Body 2 Dock User Guide

Axon Flex 2

- Axon Flex 2 Manual
- Axon Flex 2 Videos
- Axon Flex 2 Quick Start
- Axon Flex 2 Spec
- Axon Flex 2 Dock User Guide

Axon Signal

- Axon Signal Unit Manual
- ASU Spec Sheet

Docking Station

- Axon Dock Mounting Schematic
- Axon Dock Quick Start
- E-Dock 6 Bay Sec
  - Evidence.com Dock Installation Guide
  - Evidence.com Dock Wall Bracket Reference Guide V3

Documentation

- Axon Body Quick Start
- Axon Body User Manual
- Axon Deployment Guide
- Axon Flex User Manual
- Axon Flex Quick Start
- Axon Body 2 Quick Start
- Axon Dock Quick Start
- Evidence.com Admissibility and Chain of Custody
- Evidence.com and Evidence Sync Requirements
- Evicence.com Installation Guide
- Evidence.com Dock Quick Install Guide
- Evidence.com Security
- Reporting Instructions

Mobile

- Axon Capture App Guide for Android
- Axon Capture App Guide for iOS
- Axon View 4.0 for Android App Guide
- Axon View 4.0 for iOS App Guide
- Axon View Deployment Training Guide

Axon Signal

- Signal Update Guide

Security Documentation Folder

This folder contains documentation related to Security and is intended for Agency Head/Program Administrator roles.

Training Materials Folder

This folder contains Training documentation in various formats and is intended for use by Trainers, Agency Head/Program Administrator roles.

2016 Deployment Presentations

- Axon Body 2 (PowerPoint)
- Axon Flex (PDF)
- Axon Flex Training Agenda (PowerPoint)
- Intro Video for Deployments (mp4)

2016 Lesson Plans

- Lesson Plans & Course Outlines
  - Train-the-Trainer (PDF)
  - User Training (PDF)

Axon Training Videos (mp4)

- 16 videos and examples for training and reference

Product Help & Training Videos (mp4)

Short and easy to follow step-by-step instructional videos illustrating how to perform virtually any task in Evidence.com.

- 50+ videos

Reference Materials

This folder contains Training documentation in various formats and is intended for use by Trainers, Agency Head/Program Administrator roles.

- Evidence.com Administrator and Reference Guide (PDF) – also available in the "Help" section of Evidence.com
- Evidence Import Users (Excel)
- Implementation Best Practices (Word Doc)
- Roles and Permissions Chart (Excel)

Performance Measures & Service Levels

TASER utilizes performance measures throughout all phases of the project. Performance measures are based on meeting particular goals that are detailed and agreed upon prior to implementation. Examples of these goals are indicated in the Implementation Plan and User Acceptance Testing documentation attached with this response. When the FLPD determines how it would like to design the solution, this documentation will be customized and submitted to the FLPD for approval.

Implementation Performance Measures

- The FLPD accepts customized project plan
- Delivery of Hardware
- Responsiveness of Account/Sales Representative
- Responsiveness of Account Manager
- TASER meets all milestones by the date in the project plan

Training Performance Measures

- System administrators demonstrate working knowledge of the system
- System administrators demonstrate ability to configure the solution
- End users demonstrate working knowledge of the system
- End users demonstrate working knowledge of camera function

Go-Live Performance Measures

- Integration (if applicable)
- User Acceptance Testing completed and passed
- Officers using solution in field by “Go-Live” date specified in the Project Plan

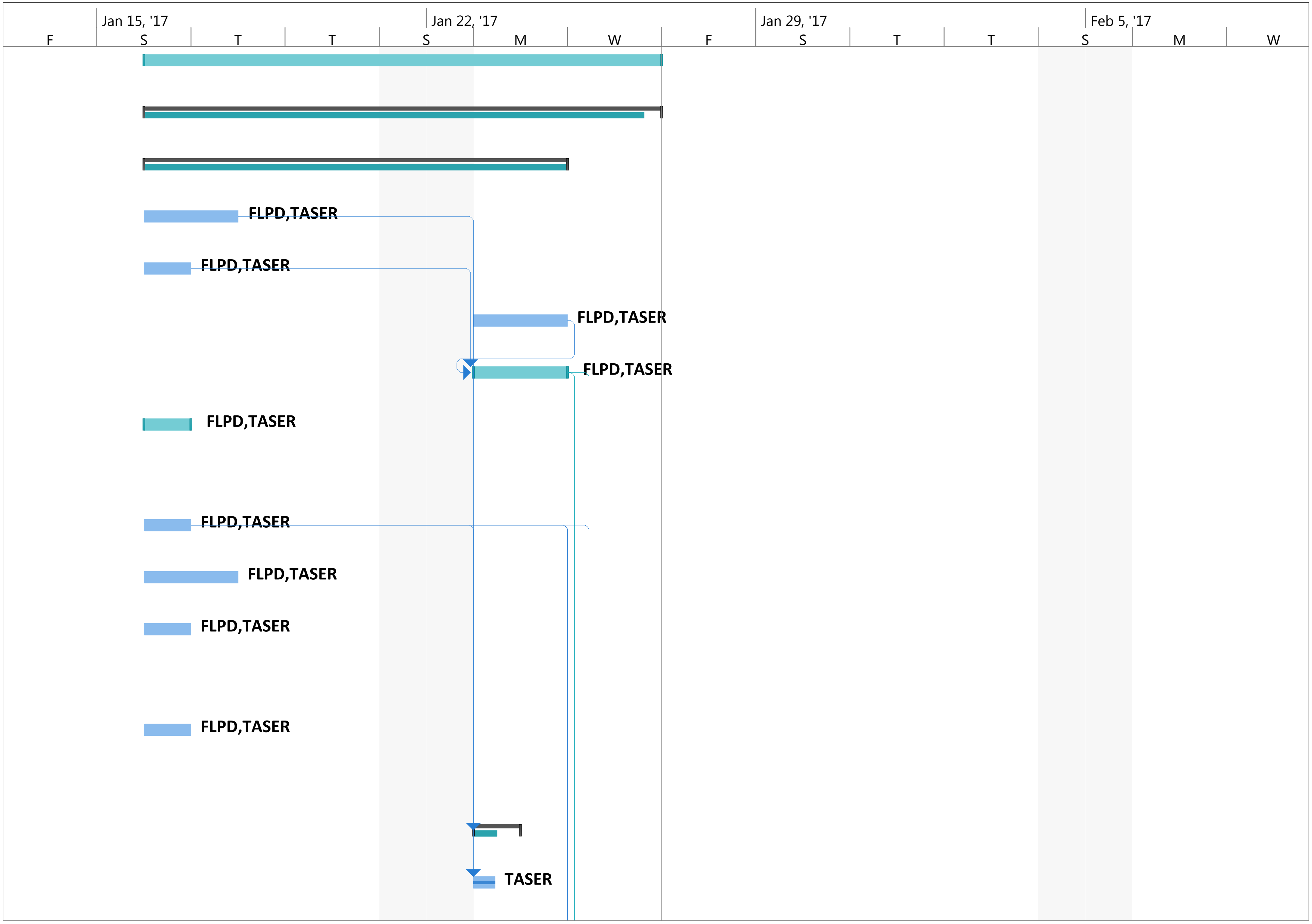
Support Performance Measures

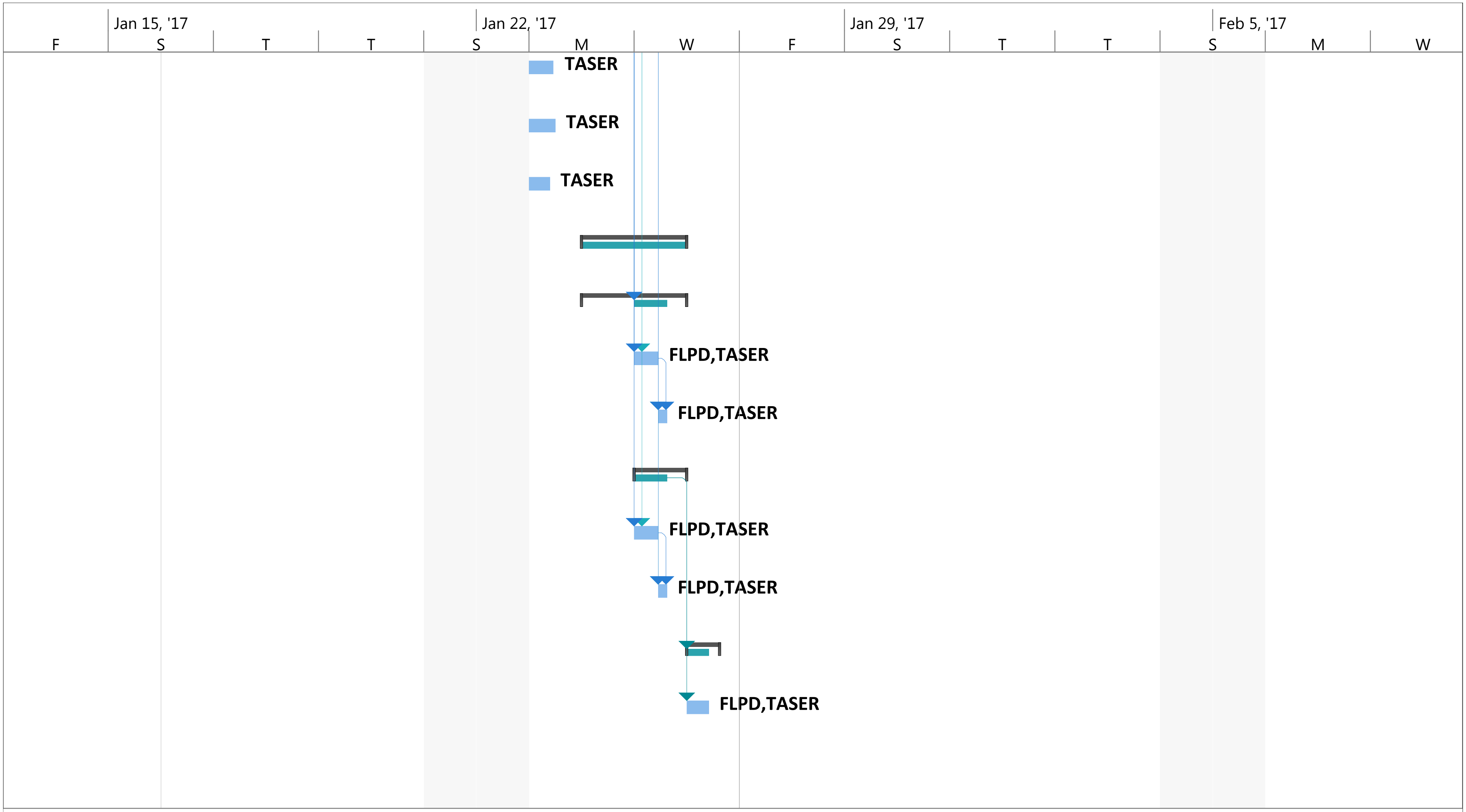
- Evidence.com uptime
- TASER meets response time indicated in the Service Level Agreement signed off on by both parties
- TASER releases Evidence.com updates on monthly cadence

Our Service Level Agreement is included in Tab 8b.

ID	Task Name	Start	Finish	Duration	Predecessors	Resource Names	W
1	**Fort Lauderdale PD Axon Project - 35**	**Mon 1/16/17**	**Thu 1/26/17**	**9 days**			
2	**Fort Lauderdale PD**	**Mon 1/16/17**	**Thu 1/26/17**	**9 days**			
3	**Configuration Tasks**	**Mon 1/16/17**	**Tue 1/24/17**	**7 days**		**FLPD,TASER**	
4	Draft Deployment Plan created	Mon 1/16/17	Tue 1/17/17	2 days		FLPD,TASER	
5	Site survey for ETM installation, test bandwidth	Mon 1/16/17	Mon 1/16/17	1 day		FLPD,TASER	
6	ETM registration and configuration	Mon 1/23/17	Tue 1/24/17	2 days		FLPD,TASER	
7	Install and test E.com Docks	Mon 1/23/17	Tue 1/24/17	2 days	5,6	FLPD,TASER	
8	Evidence.com Setup (Roles & Permissions, Categories)	Mon 1/16/17	Mon 1/16/17	1 day		FLPD,TASER	
9	Create user accounts in Evidence.com	Mon 1/16/17	Mon 1/16/17	1 day		FLPD,TASER	
10	Inventory, assign, test all Axon devices	Mon 1/16/17	Tue 1/17/17	2 days		FLPD,TASER	
11	Install AXON Mobile & Evidence Mobile App (Done at the time of training)	Mon 1/16/17	Mon 1/16/17	1 day		FLPD,TASER	
12	Install MDT Application (SYNC) (Can be done at the time of training, IT needed)	Mon 1/16/17	Mon 1/16/17	1 day		FLPD,TASER	
13	**EVIDENCE.COM Training**	**Mon 1/23/17**	**Mon 1/23/17**	**1 day**	**4**	**FLPD,TASER**	
14	Evidence.com Super User Training Session 1	Mon 1/23/17	Mon 1/23/17	3 hrs	9	TASER	

ID	Task Name	Start	Finish	Duration	Predecessors	Resource Names	W
15	Evidence.com Super User Training Session 2 (Optional)	Mon 1/23/17	Mon 1/23/17	3 hrs		TASER	
16	Train The Trainer	Mon 1/23/17	Mon 1/23/17	4 hrs		TASER	
17	Evidence Tech Training	Mon 1/23/17	Mon 1/23/17	1.5 hrs		TASER	
18	**Fort Lauderdale Go Live Rollout (35 Units)**	**Tue 1/24/17**	**Wed 1/25/17**	**2 days**		**FLPD,TASER**	
19	**Wave 1 Training**	**Tue 1/24/17**	**Wed 1/25/17**	**2 days**	**9**		
20	Gear Fit and Training - First Shift	Wed 1/25/17	Wed 1/25/17	3 hrs	7,9	FLPD,TASER	
21	Gear Fit and Training - Second Shift	Wed 1/25/17	Wed 1/25/17	3 hrs	7,9,20	FLPD,TASER	
22	**Make up Training**	**Wed 1/25/17**	**Wed 1/25/17**	**1 day**			
23	Gear Fit and Training- First Shift	Wed 1/25/17	Wed 1/25/17	3 hrs	7,9	FLPD,TASER	
24	Gear Fit and Training- Second Shift	Wed 1/25/17	Wed 1/25/17	3 hrs	7,9,23	FLPD,TASER	
25	**PIRSA Go Live Complete**	**Thu 1/26/17**	**Thu 1/26/17**	**0.75 days**	**22**		
26	Post Deployment Meeting	Thu 1/26/17	Thu 1/26/17	2 hrs	22	FLPD,TASER	
27							


Jan 15, '17
Jan 22, '17
Jan 29, '17
Feb 5, '17
F
S
T
T
S
M
W
F
S
T
T
S
M
W
FLPD,TASER
FLPD,TASER
FLPD,TASER
FLPD,TASER
FLPD,TASER
FLPD,TASER
FLPD,TASER
FLPD,TASER
FLPD,TASER
TASER


Jan 15, '17
Jan 22, '17
Jan 29, '17
Feb 5, '17
F
S
T
T
S
M
W
F
S
T
T
S
M
W
TASER
TASER
TASER
FLPD,TASER
FLPD,TASER
FLPD,TASER
FLPD,TASER
FLPD,TASER

Project Team Qualifications

TASER's project team is comprised of individuals with experience in law enforcement and in supporting our law enforcement partners worldwide. Our most experienced and skilled personnel will be involved in the implementation, development, deployment, management, and support of the FLPD's body-worn camera and digital evidence management program. With more than 154,000 cameras in the field, TASER has the experience to evaluate the FLPD's unique situation and deploy personnel as necessary. The FLPD will have access to TASER's personnel throughout the life of the project to ensure that the FLPD's deployment is completed successfully and on time.

The following TASER personnel may be involved in some part of the demonstrations, pilot, implementation, set up, follow up and support of your Axon and Evidence.com program. All of these individuals, and others, work together to be an unbeatable team when it comes to the implementation of Axon cameras and Evidence.com including the day to day service and support expected by the FLPD.

TASER Regional Support Management Team

The Regional Support Management team's primary purpose is to ensure good standing health for the FLPD's Axon and Evidence.com program, and providing the necessary resources needed to make sure agencies are set up for success. The Regional Support team members accomplish their mission utilizing consistent communication and can be reached 24 hours a day, 7 days a week.

TASER's Regional Support Managers act as primary points of support for customers to ensure positive and successful engagement with their Axon & Evidence.com deployment. As an expert on all Axon products & services, your Regional Support Manager will uncover and maintain an understanding of your goals, pain points, and drivers to improve your agency's customer experience. As updates and features are released, your Regional Support Manager will troubleshoot all changes to ensure a successful experience for customers.

The following TASER personnel will be available to lead the implementation, set-up, follow-up and support of your Axon and Evidence.com program for **Phase II – Pilot Program (Deployment).**

Chris Baker, Sr. Regional Support Manager

Chris is the Sr. Regional Support Manager and supplemental point of contact within TASER headquarters. In addition to managing the Regional Support team, his job is to ensure a good standing health for your agency's Axon and Evidence.com program by utilizing consistent communication, virtual support, and providing the necessary resources needed to make sure you are set up for success. Chris has been with TASER since January 2013 and is also the Regional Support Manager for the Southeastern US, including Florida, Georgia, North Carolina and Alabama. He is based out of TASER HQ in Scottsdale, AZ.

Pre-Sales System Engineers

TASER's Pre-Sales System Engineers are subject matter experts in the area of Software as a Service (SaaS), embedded systems, and networking, leveraging TASER International's Evidence.com and Axon body-worn camera systems. As members of the TASER sales team, the Sales Engineers support the campaign to provide on-officer evidence capture devices and SaaS solutions to more than 15,000 police departments in the United States and abroad.

Uriel Halioua, Senior Pre-Sales System Engineer

Uri is a Subject Matter Expert ("SME") on body-worn video, digital evidence capture devices, and TASER's Axon body-worn video cameras as well as Evidence.com and other forms of digital evidence management. He conducts customer site assessments, including network, electrical, and physical assessments. He also provides pre-sales engineering support to both the domestic and international sales teams.

TASER Professional Services Team

In the past 12 months, TASER's experienced Professional Services Team has completed over 211 deployments and has conducted 830 trials and evaluations.

The following TASER Professional Services personnel will be available to lead the implementation, set-up, follow-up and support of your Axon and Evidence.com program for **Phase III – Additional Purchase (Anticipated Full Deployments).**

Charles Foster, Lead Manager, Technical Services

Charles first started at TASER International in March 2004 in the IT Department and advanced to National Field Services Manager until he left the company in 2009. During his previous tenure with TASER, Charles was involved in implementing countless CEW programs both domestically and internationally as well as assisting in creating and teaching the Technical Services and Investigations Course formerly known as the Armorer's Course. He holds a Bachelor of Science in Network and Communications Management from DeVry University, has been in the Military since 2010, and is currently a First Lieutenant in the United States Army Reserve. Charles is based out of TASER headquarters in Scottsdale, AZ.

CHRISTOPHER BAKER

480-463-2130 · cbaker@taser.com

PROFESSIONAL EXPERIENCE

TASER International

Senior Regional Support Manager — September 2016-Present

- Manage team of Regional Support Managers (RSM) to ensure world class training and support on the Axon video system and Evidence.com
- Implement processes and procedures for RSM team to accomplish team and company objectives
- Manage the success of trial Evidence.com programs at police departments and sheriff offices in the Southeast Region.

Regional Support Manager — January 2013-September 2016

- Direct the implementation of AXON video system and EVIDENCE.com digital evidence maintenance software program in over 175 police departments and sheriff's offices in 22 states.
- Report status and condition of current customers directly to company executives.
- Gather feedback from law enforcement officers from across the country and work directly with product developers to improve existing products.

Phoenix Suns

Game Night Basketball Communications Staff — October 2009 – April 2014

- Train new Game Night Communication Staff members.
- Record and transcribe interviews with players and coaches.
- Collect and compile team statistics.
- Create and distribute statistical information packets that are distributed to all 30 teams along with local and national media.
- Direct interaction with Suns and visiting players as well as local, visiting, and national media.

Phoenix Mercury

Basketball Communications Assistant — March 2010 – April 2012

- Managed and directed the Game Night Communications Staff as well as the Al McCoy Media Center and press room during over 50 Phoenix Mercury games.
- Trained new Game Night Staff members.
- Created and edited team Media Guide and team Postseason Guide.
- Analyzed statistics to determine trends and tendencies as well as updated, tracked, and distributed team statistics and trends.
- Facilitated press conferences between home and visiting teams with ESPN.

INTERNSHIP EXPERIENCE

Wealth Management Intern,

Merrill Lynch, Mesa, AZ — Summer 2012

- Researched over 100 different companies, bonds, and mutual funds for company information, levels of potential risk, historical returns, and related current events to determine potential new investment opportunities and reported assessment and possible strategies to a Merrill Lynch Vice President.
- Participated in daily brainstorming exercises to think of creative ways to fix everyday problems and create new business solutions.

VOLUNTEER WORK

Hospice of the Valley; Patient Volunteer — March 2012 - Present

- Visit and provide emotional and physical aid to terminally ill patients on a weekly basis.

EDUCATION

Bachelor of Science; Finance — **Graduation: December 2012**

W. P. Carey School of Business at Arizona State University, Tempe, Arizona — **GPA 3.71**

Dean's List

Uriel Halioua

602-820-5408
uri@taser.com

Experience

Pre-Sales Systems Engineer

TASER International - August 2009, Present

I travel across the nation and internationally providing pre-sales support to TASER International's sales team. My role is to provide product presentations, answering technical Q&As, assessing customer capabilities and needs, and making customers fall in love with the cloud.

- Subject Matter Expert (SME) pertaining to EVIDENCE.COM and other forms of digital evidence management.
- Subject Matter Expert (SME) on on-body video, digital evidence capture devices, and TASER's AXON Flex On-Officer video capture device.
- Evangelizes EVIDENCE.COM and TASER video capture solutions.
- Evangelizes Cloud Computing and Software As A Service (SAAS) to the Law Enforcement, Federal, and Military Markets.
- Supporting TASER's Weapons and Video Evidence Sales teams in pre-assessment and closure of business opportunities.
- Engaging with technology decision makers (Chiefs of Police, Command staff, Sheriffs, Directors of IT) through technical sales presentations, solution demonstrations, technical workshops, competitive displacement, and exploratory discussions.
- Assisting in RFP/RFI responses.
- Development of custom Video Evidence solutions that do not exist within present product offering to customer’s requirements and objectives.
- Documented customer feature requests and issues, providing feedback to sales and product management.
- Presenting TASER’s technical & business value proposition at industry events.
- Transfer of industry, technical, and product knowledge to customers and colleagues.
- Proactive planning to prevent post sales issues that shorten time to revenue.
- Close interaction with product and project management to ensure development coincides with the growing needs of the customer.
- Conducting customer site assessments. This includes network, electrical, and physical assessments.
- Sole sales engineer providing pre-sales support to entire domestic and international sales teams.

System Deployment Engineer

BroadSoft - January 2008, June 2009

- Ensure the successful installation, integration, and deployment of our products in customer environments while maintaining quality and superior customer satisfaction.
- Provide technical training and product overview.
- Execute an Acceptance Test Plan with a customer representative.
- Correspond with sales engineering and product management during the installation phase.
- Identify design issues, create problem reports, and follow up with customer for resolution.
- Coordinate and execute customer upgrades.

Network Operations

Primus Telecommunications - January 2004, December 2007

- NOC Monkey

Network Operations Specialist

Sprint - January 2000, January 2003

Tech Support

RCN - January 1998, January 1998

Charles W. Foster II

(602)571-3432
cfoster@taser.com

Career Objective

Seeking a responsible position with a world class organization that will allow me to utilize my vast experience and training

Professional Profile

- Provided subject matter expertise for customer and technical support to law enforcement agencies and Military for advanced TASER products. This included product maintenance, problem-solving, trouble-shooting, and implementing proactive procedures and systems
- Recognized and sought after expert in problem-solving and troubleshooting advanced technical products
- Initiated customer and technical support practices across technical and product areas
- Planned, organized and implemented proactive procedures on advanced TASER systems
- Managed training and supervision of customer and technical support personnel
- Led 41 Military Police soldiers and 1 Combat Medic during combat operations in Kabul, Afghanistan

Professional Experience

TASER International, Scottsdale, AZ *08/2014 – Present*
Professional Services Manager

- Contributes recommendations to strategic plans and reviews, prepares and completes business plans, implements best practices for all TASER CEW and AXON products
- Maintain contact with customers, visits operational environments, conducts training, benchmarks best practices, and analyzes information and applications
- Studies, evaluates and re-designs Professional Services programs related to TASER CEW and AXON products
- Provides a level three support resource and technical advice to resolve issues related to all TASER CEW and AXON products as well as diagnosing client network problems

Appointment-plus, Scottsdale, AZ *05/2012 – 8/2014*
Major Account Manager

- Responsible for maintaining high level of major account retention by providing world class customer service
- Research and compile major account information and recommend standardization and functionality to client
- Coordinate with high level executives to facilitate account upgrades and grow Enterprise solutions
- Serve as liaison between major account clients and internal departments to include sales, client services, information technology and accounting
- Research, compile and reconcile critical major account information in order to maintain good standing with client base

Employbridge, Inc., Phoenix, AZ **03/2010 – 05/2012**
Account Manager

- Secure new accounts and expand business in existing accounts
- Prepare and present proposals to prospects and clients
- Develop and expand network of community contacts to maximize business development opportunities
- Cooperate with and engage support of operations staff to assure business is serviced successfully
- Meet and exceed monthly sales quotas
- Demonstrate the company core values, operating principles and service differentiators
- Document and maintain accurate information in database

TASER International Inc., Scottsdale, AZ **03/2004 – 11/2009**

National Field Services Manager

- Oversaw the scheduling and training of all support personnel
- Directed field service personnel who performed on-site routine services including installation, maintenance and repair
- Trained, motivated, counseled and monitored the performance of all customer and technical support department staff
- Managed all support personnel to ensure that customers are retained, satisfied and that their needs are fulfilled
- Managed resources to achieve service goals and assigned work schedules to ensure quality and timely delivery of service
- Instructed TASER Technicians Course to Law Enforcement and Military agencies Worldwide
- Developed new prospects and interacted with existing customers to increase sales of products and/or services

Military Experience

United States Army Reserve, Mesa, AZ **7/2010 – Present**

First Lieutenant, Platoon Leader

- Responsible for designing, executing and evaluating training exercises to ensure platoon can fulfill its mission
- Develop the management and leadership abilities of junior Non-Commissioned Officers
- Command, direct and lead military police units in both tactical and peacetime environments
- Prepare plans, policies and regulations pertaining to organization, training, operations and equipment of military police units and personnel for both combat and law enforcement operations
- Coordinated and implemented security parameters in collaboration with multiple foreign embassies, foreign militaries, governmental and non-governmental agencies located in Kabul, Afghanistan
- Liaison to base commander for a Forward Operating Base located in Kabul, Afghanistan for all base defense and force protection matters

Education

DeVry University, Phoenix, AZ **02/2004**
B.S., Network and Communications Management

U.S. Army Officer Candidate School, Fort Benning, GA **03/2011**

U.S. Army Military Police Basic Officer Leaders Course, **08/2011**
Fort Leonard Wood, MO

Accomplishments

Awarded TASER CEO Award for Excellence twice
Awarded Bronze Star Medal
Increased sales over 200% from previous quarter within first 90 days
Achieved highest all-time Monthly Recurring Revenue in first 30 days

Travel Costs

Travel costs are included in the Professional Services package costs.

Facility and Other Requirements

The FLPD should designate a Project Manager and an IT point of contact to oversee the project and facilitate communication with TASER implementation staff. The FLPD will also need to select an Evidence.com Super Administrator. This role does not differ from other Administrator accounts setup within the agency - it is simply the first account that is required to be set up for a new agency.

On-Site Resources

TASER will need a room dedicated to the training process while on-site. The room will need to be equipped with sound/AV equipment, a projector, and internet connectivity. For the User/Admin trainings, if a computer lab is available, that would be preferred if it can accommodate the aforementioned equipment.

Architectural Plan

The Evidence.com VMS is a multi-tenant hosted web-based cloud service based on a modern micro service architecture including a dynamic web application for evidence management and optional mobile applications for iOS and Android. The cloud service uses a variety of technologies including modern data storage systems (SQL and NOSQL based), cloud object storage, cloud compute resources, and various security tools and technologies. Evidence.com also offers a secure API platform for custom application integration and federated authentication and user management using standards-based protocols (SAML). All content stored within Evidence.com is encrypted in motion and at rest.

Evidence.com is a cloud-hosted digital evidence management solution provided as a service (SaaS) application. It is horizontally scalable and can elastically adapt to accommodate any traffic volumes. Internally, the solution uses a service oriented architecture where functionality is provided by discrete compassable services that can run on one or many servers. This allows individual components to scale to handle changes in traffic volumes.

Software is included in the purchase of Evidence.com licenses.

Software

- Evidence.com

Evidence.com is a source-agnostic digital evidence management system, allowing for digital evidence of any kind such as digital images, digital audio files, etc. Evidence.com and Evidence Sync both have UI/UX interfaces for direct upload of any digital content from a user's computer.

- Evidence Sync
  TASER's Evidence Sync software client allows connectivity to Windows based Mobile Data Terminals (MDT), Mobile Data Computers (MDC), or desktop computers. Using a USB cable, the Axon camera can be connected to any of the listed devices, allowing for annotation of captured videos with metadata, upload, and charging. Evidence Sync is provided freely to customers.

- Axon Mobile Application Suite: Axon View and Axon Capture

  Axon View is a mobile application that wirelessly connects with your Axon camera to provide instant playback of unfolding events from the field, in the field. You can use the app's live display to ensure your camera is well-placed, and the playback function helps eliminate the "he said, she said" on the spot.

  Axon Capture is an application built specifically for law enforcement that allows officers to capture digital evidence right from the field. The app eliminates the need to carry three separate devices for photo, video, and audio recording. Instead, it builds upon the capabilities already in your pocket with the security and organization needed to protect truth. You can add tags, titles or GPS coordinates to any recordings before you upload the data to Evidence.com.

Hardware

- Axon cameras, mounts and cables
  The Axon on-officer video system functions as the capture device. All videos are captured as MP4 files and should be playable in most if not all video players.

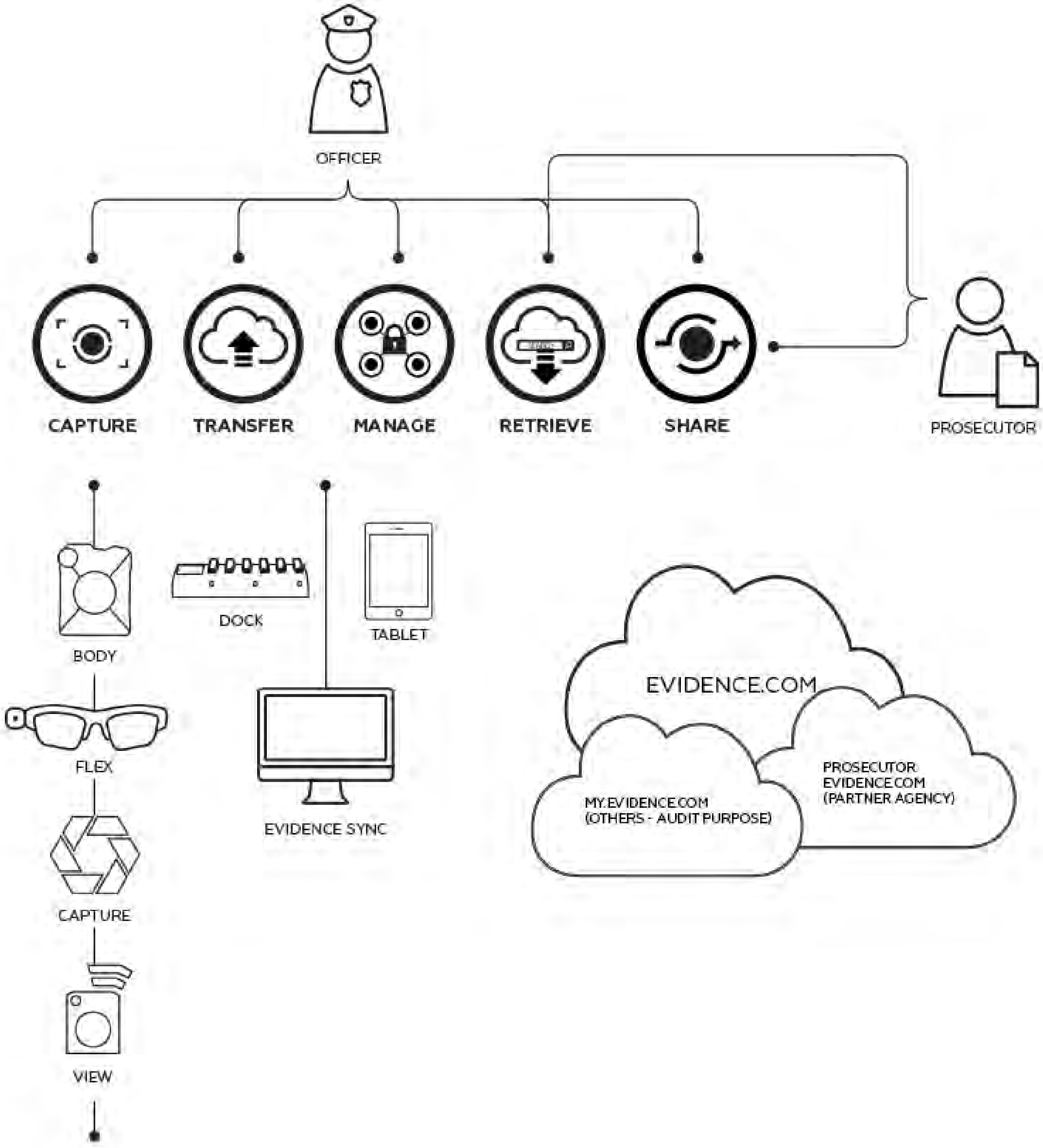
- Axon Docks
  The Axon Dock serves as the charging and upload station for the Axon camera. The docks terminate directly into the local LAN, then securely route over the Internet to Evidence.com.

Hardware and Software

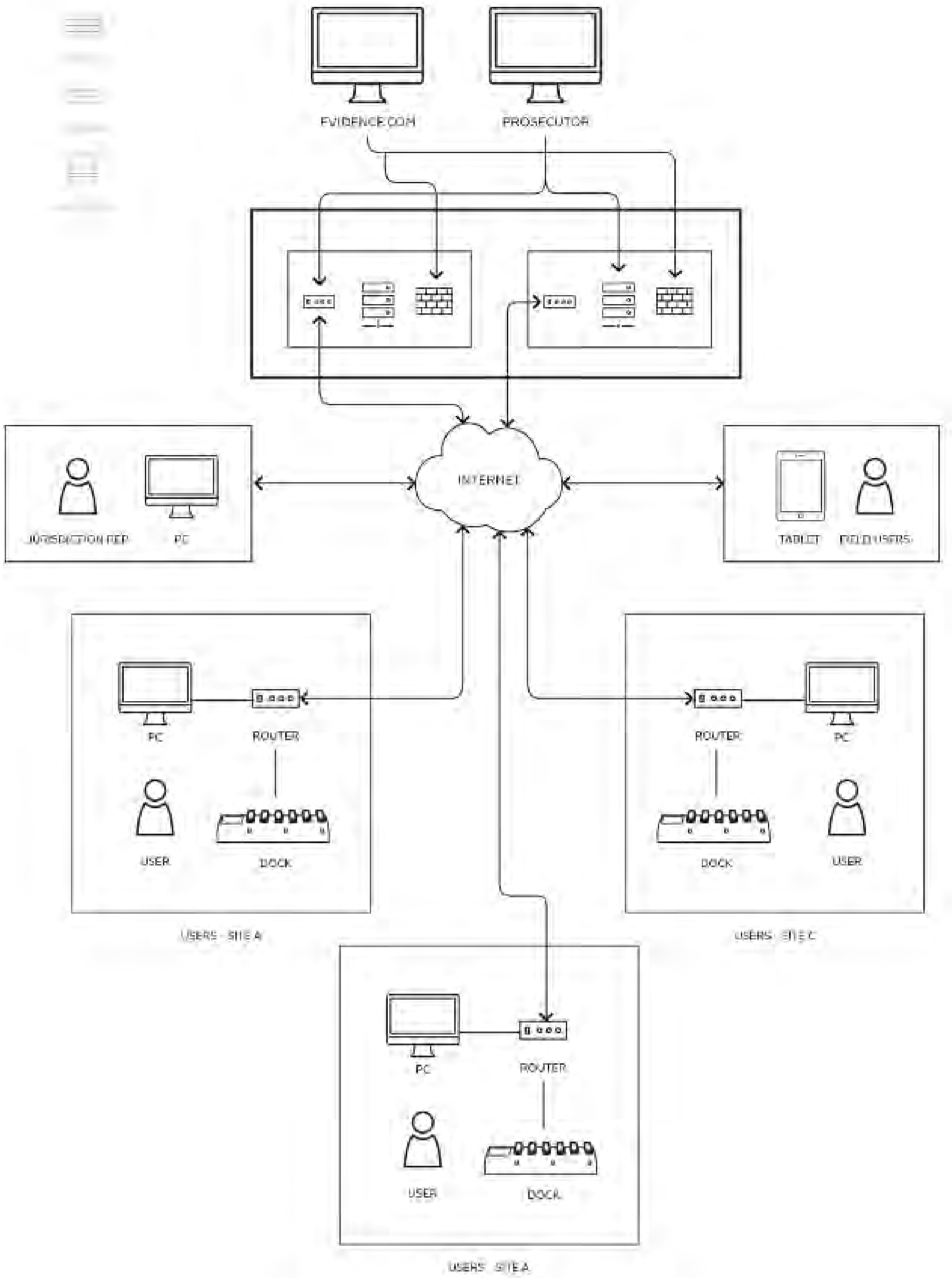
Axon hardware delivers a full turn-key-solution and is specifically designed to meet the needs of law enforcement. TASER is the sole manufacturer of the Axon and Evidence.com product lines and does not to depend on third party components and third party support.

Item	**Description**
Hardware	
Axon Flex 2	POV camera
Axon Flex 2 Controller	PS and control unit for Axon Flex system
Axon Flex 2 Mounts	Variable mounting options for Axon Flex system
Axon Flex 2 Cable	P1-P1 cable to connect Axon Flex DVR to Axon Flex Controller
Axon Flex 2 Controller Holster	Variable holster options to mount Axon Flex controller to Officer's body
Axon Body 2	2nd Gen of Axon's single-piece BWC system
Axon Body 2 Holster	Variable holster options to mount Axon Body 2 to Officer's body
Data/Power Cable	USB-P1 cable to connect Axon Camera Systems to Personal Computer/MDCs to manage Data or Charging Axon Flex Controllers
Axon Dock	Docking stations to Upload BWC Videos to Evidence.com and charging batteries automatically. Each Axon dock may have up to 6 docking bays
Software	
Evidence.com	Evidence.com is a cloud-hosted digital evidence management solution provided as a service (SaaS) application. It is horizontally scalable and can elastically adapt to accommodate any traffic volumes. Internally, the solution uses a service-oriented architecture where functionality is provided by discrete compassable services that can run on one or many servers. This allows individual components to scale to handle changes in traffic volumes. The application is designed to support uploads from multiple users, devices, and locations, simultaneously from thousands of agencies across the United States. It is also possible for concurrent users to access the same video at the same time
Evidence Sync	Software to allow secure Data upload from Personal Computer/MDCs to Evidence.com

Axon Solution Map



Evidence.com Solution Diagram



Continuity of Operations/Disaster Recovery Plan

TASER International maintains disaster recovery procedures and business continuity plans for Evidence.com. Due to the distributed nature of the application, infrastructure and data, traditional disaster recovery tests from media are not performed as the redundant operations and geographically distributed hardware are continuously tested in the course of normal business operations. Business continuity plans are tested in a table-top setting on a periodic basis.

In the event of a disaster, the system will failover automatically to the secondary site and provide uninterrupted service to customers, providing uninterrupted access during disaster events. Data centers offer world-class security, system protection, employ backup power, climate control, alarms, and seismic bracing.

All data and systems are stored in the United States and are replicated between two data centers. In the event of a disaster, the system will failover automatically to the secondary site and provide uninterrupted service to any customer system. This provides uninterrupted access during disaster events.

Information Security Policies - Cloud Hosting Policy

Security Compliance Certification

TASER deploys a comprehensive Information Security Program (ISP) to provide for the confidentiality, integrity and availability of all customer data in Evidence.com. Security is integrated throughout TASER International's products, development processes and corporate culture to ensure the security of data and maintain trust with customers. Our security program includes frequent penetration tests, static code analysis, white box testing, and designing of solutions that provide PKI-based end-to-end encryption with digital authenticity and integrity signing.

The Evidence.com Information Security program is compliant with the defined requirements of ISO/IEC 17021:2011 and ISO/IEC 27001:2013, and is rigorously reviewed and audited to ensure compliance with the CJIS Security Policy.

Evidence.com will allow the FLPD to configure granular role-based access controls to ensure only authorized individuals can view and perform authorized actions on FLPD data.

Evidence.com supports customer single sign-in (SSO) and account registration over Security Assertion Markup Language (SAML) to enable integration into existing FLPD identity services.

Security Features

Additionally, Evidence.com provides many security features and capabilities to enable customers to secure digital evidence including password complexity requirements, failed login limits, and enforced timeout settings. Multi-factor authentication (MFA) options are also configurable for user login and prior to administrative actions. MFA can use a one-time code via SMS or phone call-back to provided phone numbers. Evidence.com requires two-factor authentication for all system administration access and many has features to provide robust access control. Administration is performed over a secured VPN connection.

Passwords for system and application administration requires nine character passwords and contain at least three of the four character categories (Upper letter, Lower letter, Number, Symbol). Step-up authentication is performed using a one-time, 6-character code delivered out-of-band to a previously authenticated device.

Evidence.com safeguards the integrity and authenticity of digital evidence. Features ensure evidence meets chain-of-custody requirements and authenticity can be proven to be authentic and free from tampering in the following ways:

- Forensic fingerprint of each evidence file using industry standard SHA hash function. Integrity is validated before and after upload to ensure no changes occurred during transmission.
- Full tamper-proof audit records are created in real-time and available for FLPD review and monitoring. The evidence logs capture the when, who and what for each evidence file. These records cannot be edited or changed, even by account administrators.
- Original evidence files are never altered; even when derivative works (video segments) are created.
- Deletion protection, including deletion approval workflows, deletions notification emails, and a deletion remorse period to recover accidently deleted evidence files.

Access to Client Data

All customer access to data is controlled at layer 7 of the OSI model within the web application interface over HTTPS. Additionally, Evidence.com enables FLPD to control access at layer 4 of the OSI model by establishing IP whitelisting to define and limit the IP ranges in which an FLPD user may access Evidence.com. TASER International also protects Evidence.com at layer 4 by blacklisting known malicious IP addresses. TASER International protects and controls access on behalf of all Evidence.com customers at layer 3 of the OSI model. Customer data is uniquely identified and marked to ensure appropriate segregation of customer data.

To protect the web application, TASER International deploys a web application firewall (WAF) to actively protect against threats in real-time. Additionally, TASER International performs at least quarterly penetration testing of Evidence.com. Penetration testing includes testing to ensure customer data segregation is maintained and not commingled.

Encryption

All evidence data is encrypted at rest and in transit. Robust SSL/TLS is implemented for data in transit using TLS 1.2 with a 256 bit connection and Perfect Forward Secrecy. Evidence data stored at rest is encrypted with at least 256 bit AES.

Disaster Recovery and Continuity Plan

TASER has designed Evidence.com to be highly scalable and extremely resilient. Evidence.com customer data is stored within data centers located in Boydton, VA and Des Moines, IA. Each data center offers world-class security and system protection. All data centers employ backup power, climate control, alarms, and seismic bracing.

In the event of a disaster, the system will failover automatically to the secondary site and provide uninterrupted service to customers, providing uninterrupted access during disaster events.

The application's highly resilient architecture and application delivery is supported by the Service Level Agreement established with TASER International’s customer base.

TASER maintains a Business Continuity Plan that encompasses Evidence.com operations and resiliency capabilities. This plan is reviewed periodically and is ISO 27001certified.

Design, development and maintenance of Evidence.com is performed by TASER personnel within authorized facilities. These facilities are included in scope TASER's International Information Security Program. Design, development and maintenance are only performed in the United States. FLPD data stored within Evidence.com will remain in the United States.

TASER has developed and operates secure software development lifecycle procedures (SDLC). Execution within the SDLC ensures security is evaluated at every phase of development and that quality measures are met. TASER does not outsource the development of Evidence.com and development resources are assigned and dedicated to the on-going development, quality and security of the product.

CJIS Compliance

TASER acknowledges and abides by all aspects of the CJIS Security Addendum, and we are contractually committed to meeting CJIS, as the CJIS Security Addendum is included by reference into the Evidence.com Master Services Agreement.

All TASER CJIS-authorized personnel are required to complete CJIS security training in compliance with the CJIS Security Policy. TASER uses 'CJIS Online' from Peak Performance Solutions to conduct and coordinate CJIS-specific security training. TASER personnel training records are available to customers within the CJIS Online system. Any additional FLPD-specific security awareness training can be conducted as required.

In addition to security awareness, training, TASER CJIS-authorized personnel have undergone state and federal fingerprint based checks in certain states. TASER is prepared to coordinate with FLPD to ensure that all TASER CJIS-authorized personnel undergo checks in alignment with the requirements of the FLPD.

TASER's CJIS compliance status has been validated independently by CJIS ACE and the underlying security program is audited on at least an annual basis by an additional third party as part of TASER's ISO 27001program.

Risk Detection

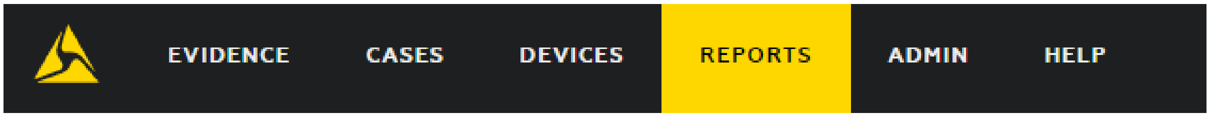
Evidence.com employs advanced detection and analysis capabilities of system events. This includes automated detection and alerts for unusual activity or attacks.

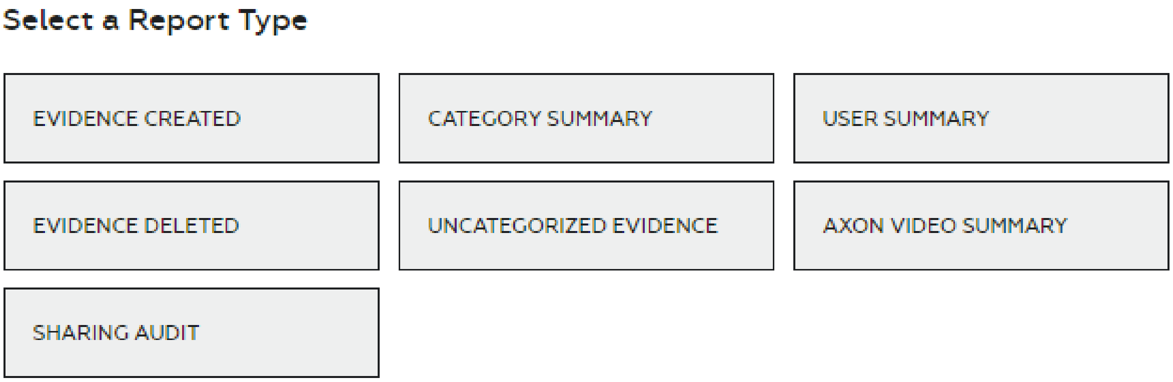
TASER International maintains a robust information security program designed to provide a high level of protection against current and emerging threats. This includes logging all access to evidence data and systems, and robust evidence audit reports within Evidence.com.

The Evidence.com infrastructure utilizes a multi-tier design that segregates the database tier from web and application tiers using firewalls and network ACLs. Evidence.com utilizes host-based firewalls on all applicable systems. Host based IDS & AV are deployed on applicable systems.

Reports

Evidence.com allows administrators and those with the reporting permission to generate reports showing Evidence.com utilization. These options can help your agency turn that data into valuable answers to ensure your Evidence.com account is providing you with the flexibility and utility your agency deserves. Evidence.com has pre-set categories; however, agencies can add customized categories based on Agency guidelines and protocols.





Report Types

- **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.
- **Evidence Deleted** — Lists all evidence deleted and associated metadata on your agency's account in order of when the data was deleted. This report will give better monitoring of automated deletions and help ensure a proper retention policy is in place.
- **Category Summary** — Lists the current count of total files and file size in megabytes (MB) for each category as well as the percent of files assigned to that category.

- **Uncategorized Evidence** — Lists users with uncategorized evidence assigned to them. A second tab on the export lists every piece of uncategorized evidence and includes the owner information, evidence title, date recorded, and link to the evidence.
- **User Summary** — Lists total files and file size in MB, broken out by owner of the evidence. The counts are further broken out by evidence type, active, and deleted evidence.
- **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 uploads by the specified grouping: Day, Month, or Year.
- **Sharing Audit Report** — The Sharing Audit report exports a list of all user actions related to sharing evidence and cases to a CSV file. You can specify the date range for the report.

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. You can download reports either by visiting the Reports page or by the download link in a notification email. Completed reports are available from the Download Queue section of the Reports page. If you have permission to run reports, you can download reports that any user has run.

Evidence.com reports are spreadsheets in an XLSX file format, which 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 of time.

Exporting Evidence Search Results for Reports

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

Evidence Search Filters

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

- **Category** — Limits search results to evidence that is assigned to the category that you select. By default, search results include evidence assigned to any category, including uncategorized evidence.
- **Date** — Limits search results by either the recorded, uploaded, or deletion date of evidence, as selected. You must also specify a date range by using the From and To boxes, else the search is not limited by date range. Search results are inclusive of the dates specified.
  1. **From** — The start of the date range. If the From box is empty, the date range begins with the earliest possible date.
  2. **To** — The end of the date range. If the To box is empty, the date range ends with today.
- **File Type** — Limits search results to the file type selected. By default, search results include all file types.
- **Owner** — Limits search results to evidence owned by the user specified. To specify the user, click in the Owner box, start typing the name of the user, wait for the system to show the matching users, and then click the user you want.
- **Uploaded By** — Limits search results to evidence uploaded by the user specified. To specify the user, click in the Uploaded By box, start typing the name of the user, wait for the system to show the matching users, and then click the user you want.

  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.

- **Tag** — Limits search results to evidence whose tags includes the characters you enter in the Tag box. For more information, see Text Search Details.
- **Group** — Limits search results to evidence owned by members of the group specified. To specify the group, click in the Group box, start typing the name of the group, wait for the system to show the matching groups, and then click the group you want.
- **Flagged** — Limits search results to evidence whose flag status matches the flag status selected.

Users can generate reports using the current version of the following browsers:

- Microsoft Internet Explorer
- Google Chrome
- Mozilla Firefox
- Apple Safari

Evidence.com Partner API

The Evidence.com Partner API provides a programmatic means to access the data in your Evidence.com agency. By developing API-compliant client software or using third-party client software, you can use the Partner API to integrate your Evidence.com agency with other systems. An API client can request create, read, update, and delete operations on a variety of data resources such as reports.

By using the Partner API, you can address your agency's specific operational needs.

The API provides the means to achieve customized ends, such as Customized Reporting. When your agency needs to audit user behavior for policy compliance, such as timely application of critical metadata, the Evidence.com dashboard and reports may not support the precise need. Through the Partner API, you can retrieve the necessary user and evidence data and provide it to the application or system that will perform custom analysis in support of your policies.

Return Policy

Return Material Authorization Procedure

The Return Material Authorization (RMA) department is located at the TASER International Headquarters in Scottsdale, Arizona, USA. The RMA department prioritizes returned products for analysis and/or repair on a First-In-First-Out (FIFO) basis, based on the severity of the complaint (or unless otherwise requested by the agency). The general turn-around-time for a full resolution is less than 14 calendar days from receipt of the returned product.

Agencies are required to submit a request for repair/replacement via the TASER RMA website and are responsible for all shipping costs (unless already agreed upon in advance). Upon receipt of them item(s), the RMA department will conduct a failure analysis investigation to determine the root cause of the issue and repair the item if possible. It is at TASER's sole discretion to repair or replace a device as identified in the original manufacturer warranty and/or extended warranty policy.

Standard Manufacturer Warranty

TASER warrants that its law enforcement hardware products are free from defects in workmanship and materials for a period of one (1) year from the date of receipt. TASER-Manufactured Accessories are covered under a limited 90-day warranty from the date of receipt. Non-TASER manufactured accessories are covered under the manufacturer's warranty.

Extended Warranty

There are extended warranties available, which will cover the hardware for 3 years total (1 year manufacturer's warranty plus 2 years extended).

The TASER Assurance Plan (TAP)

The TASER Assurance Plan (TAP) includes the extended warranty coverage described above, as well as spare products and upgraded models at the end of the TAP Term. The TASER Assurance Plan (TAP) is bundled into the purchase price of the Ultimate and Unlimited Plan Evidence.com licenses. The TAP includes Axon camera upgrades every 2.5 years, TASER's extended warranty and spare cameras.

The TASER Assurance Plan (TAP) includes the extended warranty coverage described in the current hardware warranty, as well as spare products and upgraded models at the end of the TAP Term. TAP does not apply to software or services offered for, by, on, or through the TASER.com or Evidence.com websites. You may not have both an optional extended warranty and TAP on Axon products.

Software Upgrades and Updates

The latest product features and enhancements are included as part of your investment in Evidence.com. Software is updated regularly throughout the year, and these updates are included in the price of your software licenses.

TASER's Cost Proposal (provided under separate cover) includes options for the TASER Assurance Plan warranty coverage.

Please see the TASER Master Services and Purchasing Agreement included in Tab 8b, which outlines the full terms and conditions of the standard manufacturer warranty, extended warranty and TASER Assurance Plan.

REFERENCES

BEGIN CONFIDENTIAL INFORMATION

1. **Orange County, FL Sheriff's Office**
   2500 W. Colonial Dr. 1st Floor
   Orlando, FL 32804

   Vicki Bickford, (407)254-7270 ext. 70798, Vicki.Bickford@ocfl.net

   - **Date**: March 2015 – November 2015 (Trial through deployment)
   - **Total / Type of camera used**: 660 Axon Flex cameras
   - **Currently storing data per year**: Unlimited Storage
   - **Date cameras were deployed**: August 2015 Total cost of the project
   - **Contract amount**: $3.3mm over five years

2. **Broward County, FL Sheriff's Office**
   2601 W. Broward Blvd
   Ft Lauderdale, FL 33312

   Sergeant Kevin McClure, 954-831-8741 (Desk), Kevin_Mcclure@sheriff.org

   - **Date**: March 2016-September 2016 (Trial to Deployment)
   - **Total / Type of camera used**: Up to 1,500 Axon Body 2 cameras
   - **Currently storing data per year**: 17TB per year is the average
   - **Date cameras were deployed**: September 2016
   - **Contract amount**: $5.7mm over five years

3. **Pasco County, FL Sheriff's Office**
   20101 Central Blvd
   Land O' Lakes, FL 34637

   Lt. Robert Gartnberg, (813) 235-6180, rgartenberg@pascosheriff.org

   - **Date**: August 2014-March 2015 (Trial through phased deployment)
   - **Total / Type of camera used**: 415 Axon Flex cameras
   - **Currently storing data per year**: Unlimited Storage
   - **Date cameras were deployed**: December 2014
   - **Contract amount**: $2mm over five years

END CONFIDENTIAL INFORMATION

M/WBE PARTICIPATION / SUBCONTRACTORS

If your firm is a certified minority business enterprise as defined by the Florida Small and Minority Business Assistance Act of 1985, provide copies of your certification(s). If your firm is not a certified M/WBE, describe your company's previous efforts, as well as planned efforts in meeting M/WBE procurement goals under Florida Statutes 287.09451.

TASER is not a certified minority business enterprise. TASER makes all good-faith efforts to research and acquire MBE / WBE firms, subcontractors, consultants and employees as needed to successfully complete our projects. Because TASER is the sole manufacturer of the Axon and Evidence.com product lines, it has not been a necessity to hire outside entities or subcontractors.

Since TASER performs every portion of the system implementation as well as on-going support, this methodology will add simplicity to the execution of your program, as you will only need to work with one vendor to get your entire system up and running. This adds value and cost benefits to your project and department due to the consistency of one company successfully managing and coordinating your project.

SUBCONTRACTORS

Proposer must clearly identify any subcontractors that may be utilized during the term of this contract.

We (TASER) are the sole manufacturer of the Axon and Evidence.com product lines and therefore do not subcontract outside entities.

AIA® Document A310™ – 2010

Bid Bond

N/A

CONTRACTOR:
(Name, legal status and address)
TASER INTERNATIONAL, INC.
17800 North 85th Street
Scottsdale, AZ 85255

SURETY:
(Name, legal status and principal place of business)
ARCH INSURANCE COMPANY
300 Plaza Three
Jersey City, NJ 07311-1107

OWNER:
(Name, legal status and address)
CITY OF FT. LAUDERDALE, FL
Finance Department / Procurement Services Division
100 N. Andrews Ave., Room 619, Ft. Lauderdale, FL 33301-1016

BOND AMOUNT: Thirty Thousand and 00/100 Dollars
($ 30,000.00)

PROJECT:
(Name, location or address, and Project number, if any)
Wearable Body Cameras (Cameras), a Digital Evidence Management System (System), and the accessories and ancillary components.

Project Number, if any: N/A

This document has important legal consequences. Consultation with an attorney is encouraged with respect to its completion or modification.

Any singular reference to Contractor, Surety, Owner or other party shall be considered plural where applicable.

The Contractor and Surety are bound to the Owner in the amount set forth above, for the payment of which the Contractor and Surety bind themselves, their heirs, executors, administrators, successors and assigns, jointly and severally, as provided herein. The conditions of this Bond are such that if the Owner accepts the bid of the Contractor within the time specified in the bid documents, or within such time period as may be agreed to by the Owner and Contractor, and the Contractor either (1) enters into a contract with the Owner in accordance with the terms of such bid, and gives such bond or bonds as may be specified in the bidding or Contract Documents, with a surety admitted in the jurisdiction of the Project and otherwise acceptable to the Owner, for the faithful performance of such Contract and for the prompt payment of labor and material furnished in the prosecution thereof; or (2) pays to the Owner the difference, not to exceed the amount of this Bond, between the amount specified in said bid and such larger amount for which the Owner may in good faith contract with another party to perform the work covered by said bid, then this obligation shall be null and void, otherwise to remain in full force and effect. The Surety hereby waives any notice of an agreement between the Owner and Contractor to extend the time in which the Owner may accept the bid. Waiver of notice by the Surety shall not apply to any extension exceeding sixty (60) days in the aggregate beyond the time for acceptance of bids specified in the bid documents, and the Owner and Contractor shall obtain the Surety's consent for an extension beyond sixty (60) days.

If this Bond is issued in connection with a subcontractor's bid to a Contractor, the term Contractor in this Bond shall be deemed to be Subcontractor and the term Owner shall be deemed to be Contractor.

When this Bond has been furnished to comply with a statutory or other legal requirement in the location of the Project, any provision in this Bond conflicting with said statutory or legal requirement shall be deemed deleted herefrom and provisions conforming to such statutory or other legal requirement shall be deemed incorporated herein. When so furnished, the intent is that this Bond shall be construed as a statutory bond and not as a common law bond.

Signed and sealed this 19th day of October, 2016

TASER INTERNATIONAL, INC.
(Principal) *(Seal)*

(Witness)

(Title)

ARCH INSURANCE COMPANY
(Surety) *(Seal)*

Jeni Bromberek
(Witness) Jeni Bromberek

Marina Tapia
(Title) Marina Tapia, Attorney in Fact

CALIFORNIA ALL-PURPOSE ACKNOWLEDGMENT

A Notary Public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California

County of Los Angeles

On OCT 1 9 2016 before me, Bernadette Aleman, Notary Public, personally appeared Marina Tapia who proved to me on the basis of satisfactory evidence to be the person(~~s~~) whose name(~~s~~) is/~~are~~ subscribed to the within instrument and acknowledged to me that ~~he~~/she/~~they~~ executed the same in ~~his~~/her/~~their~~ authorized capacity(~~ies~~), and that by ~~his~~/her/~~their~~ signature(~~s~~) on the instrument the person(~~s~~), or the entity upon behalf of which the person(~~s~~) acted, executed the instrument.

NR01
BERNADETTE ALEMAN
COMM. #2162246
Notary Public - California
Los Angeles County
My Comm. Expires Aug. 7, 2020
NR01

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

Signature

Signature of Notary Public

AIC 0000187173

THIS POWER OF ATTORNEY IS NOT VALID UNLESS IT IS PRINTED ON BLUE BACKGROUND.

This Power of Attorney limits the acts of those named herein, and they have no authority to bind the Company except in the manner and to the extent herein stated. Not valid for Mortgage, Note, Loan, Letter of Credit, Bank Deposit, Currency Rate, Interest Rate or Residential Value Guarantees.

POWER OF ATTORNEY

Know All Persons By These Presents:

That the Arch Insurance Company, a corporation organized and existing under the laws of the State of Missouri, having its principal administrative office in Jersey City, New Jersey (hereinafter referred to as the "Company") does hereby appoint:

Edward C. Spector, James Ross, KD Conrad, Marina Tapia, Simone Gerhard, Tom Branigan and Tracy Aston of Los Angeles, CA (EACH)

its true and lawful Attorney(s)in-Fact, to make, execute, seal, and deliver from the date of issuance of this power for and on its behalf as surety, and as its act and deed:

Any and all bonds, undertakings, recognizances and other surety obligations, in the penal sum not exceeding Ninety Million Dollars ($90,000,000.00).

This authority does not permit the same obligation to be split into two or more bonds In order to bring each such bond within the dollar limit of authority as set forth herein.

The execution of such bonds, undertakings, recognizances and other surety obligations in pursuance of these presents shall be as binding upon the said Company as fully and amply to all intents and purposes, as if the same had been duly executed and acknowledged by its regularly elected officers at its principal administrative office in Jersey City, New Jersey.

This Power of Attorney is executed by authority of resolutions adopted by unanimous consent of the Board of Directors of the Company on September 15, 2011, true and accurate copies of which are hereinafter set forth and are hereby certified to by the undersigned Secretary as being in full force and effect:

"VOTED, That the Chairman of the Board, the President, or the Executive Vice President, or any Senior Vice President, of the Surety Business Division, or their appointees designated in writing and filed with the Secretary, or the Secretary shall have the power and authority to appoint agents and attorneys-in-fact, and to authorize them subject to the limitations set forth in their respective powers of attorney, to execute on behalf of the Company, and attach the seal of the Company thereto, bonds, undertakings, recognizances and other surety obligations obligatory in the nature thereof, and any such officers of the Company may appoint agents for acceptance of process."

This Power of Attorney is signed, sealed and certified by facsimile under and by authority of the following resolution adopted by the unanimous consent of the Board of Directors of the Company on September 15, 2011:

VOTED, That the signature of the Chairman of the Board, the President, or the Executive Vice President, or any Senior Vice President, of the Surety Business Division, or their appointees designated in writing and filed with the Secretary, and the signature of the Secretary, the seal of the Company, and certifications by the Secretary, may be affixed by facsimile on any power of attorney or bond executed pursuant to the resolution adopted by the Board of Directors on September 15, 2011, and any such power so executed, sealed and certified with respect to any bond or undertaking to which it is attached, shall continue to be valid and binding upon the Company.

In Testimony Whereof, the Company has caused this instrument to be signed and its corporate seal to be affixed by their authorized officers, this 19th day of May, 2016.

Attested and Certified

Arch Insurance Company

Patrick K Nail

Patrick K. Nails, Secretary

Arch Insurance Company
CORPORATE
SEAL
1971
Missouri

David Finkelst

David M. Finkelstein, Executive Vice President

STATE OF PENNSYLVANIA SS

COUNTY OF PHILADELPHIA SS

I, Helen Szafran, a Notary Public, do hereby certify that Patrick K. Nails and David M. Finkelstein personally known to me to be the same persons whose names are respectively as Secretary and Executive Vice President of the Arch Insurance Company, a Corporation organized and existing under the laws of the State of Missouri, subscribed to the foregoing instrument, appeared before me this day in person and severally acknowledged that they being thereunto duly authorized signed, sealed with the corporate seal and delivered the said instrument as the free and voluntary act of said corporation and as their own free and voluntary acts for the uses and purposes therein set forth.

COMMONWEALTH OF PENNSYLVANIA
NOTARIAL SEAL
HELEN SZAFRAN, Notary Public
City of Philadelphia, Phila. County
My Commission Expires October 3, 2017

Helen Szafran

Helen Szafran, Notary Public
My commission expires 10/03/2017

CERTIFICATION

I, Patrick K. Nails, Secretary of the Arch Insurance Company, do hereby certify that the attached Power of Attorney dated May 19, 2016 on behalf of the person(s) as listed above is a true and correct copy and that the same has been in full force and effect since the date thereof and is in full force and effect on the date of this certificate; and I do further certify that the said David M. Finkelstein, who executed the Power of Attorney as Executive Vice President, was on the date of execution of the attached Power of Attorney the duly elected Executive Vice President of the Arch Insurance Company.

IN TESTIMONY WHEREOF, I have hereunto subscribed my name and affixed the corporate seal of the Arch Insurance Company on this _______day of OCT 1 9 2016 20____.

Patrick K Nail

Patrick K. Nails, Secretary

This Power of Attorney limits the acts of those named therein to the bonds and undertakings specifically named therein and they have no authority to bind the Company except in the manner and to the extent herein stated.

PLEASE SEND ALL CLAIM INQUIRIES RELATING TO THIS BOND TO THE FOLLOWING ADDRESS:

Arch Insurance – Surety Division
3 Parkway, Suite 1500
Philadelphia, PA 19102

Arch Insurance Company
CORPORATE
SEAL
1971
Missouri

BID/PROPOSAL CERTIFICATION

Please Note: If responding to this solicitation through BidSync, the electronic version of the bid response will prevail, unless a paper version is clearly marked **by the bidder** in some manner to indicate that it will supplant the electronic version. All fields below must be completed. If the field does not apply to you, please note N/A in that field.

If you are a foreign corporation, you may be required to obtain a certificate of authority from the department of state, in accordance with Florida Statute §607.1501 (visit http://www.dos.state.fl.us/).

Company: (Legal Registration) TASER International, Inc.

Address: 17800 N. 85th Street City: Scottsdale State: AZ Zip: 85255

Telephone No. 800-978-2737 FAX No. 480-905-2000 Email: contracts@taser.com

Delivery: Calendar days after receipt of Purchase Order **(section 1.02 of General Conditions)**: 4-8 weeks ARO

Total Bid Discount **(section 1.05 of General Conditions)**: TASER's proposed pricing includes various discounts on each of the quotes included in the cost proposal. In order to remain compliant with the bid/proposal instructions, percentage discount amounts are included on page 2 of the separate, sealed Cost Proposal and the discounted dollar amounts are reflected in each quote.

Does your firm qualify for MBE or WBE status **(section 1.09 of General Conditions)**: MBE N/A WBE N/A

ADDENDUM ACKNOWLEDGEMENT - Proposer acknowledges that the following addenda have been received and are included in the proposal:

Addendum No.	Date Issued	Addendum No.	Date Issued	Addendum No.	Date Issued
1	10/03/2016	3	10/18/2016	5	10/27/2016
2	10/14/2016	4	10/26/2016	6	10/28/2016

VARIANCES: If you take exception or have variances to any term, condition, specification, scope of service, or requirement in this competitive solicitation you must specify such exception or variance in the space provided below or reference in the space provided below all variances contained on other pages within your response. Additional pages may be attached if necessary. No exceptions or variances will be deemed to be part of the response submitted unless such is listed and contained in the space provided below. The City does not, by virtue of submitting a variance, necessarily accept any variances. If no statement is contained in the below space, it is hereby implied that your response is in full compliance with this competitive solicitation. If you do not have variances, simply mark N/A. **If submitting your response electronically through BIDSYNC you must also click the "Take Exception" button.**

Please see the attached exceptions on the following page.

The below signatory hereby agrees to furnish the following article(s) or services at the price(s) and terms stated subject to all instructions, conditions, specifications addenda, legal advertisement, and conditions contained in the bid/proposal. I have read all attachments including the specifications and fully understand what is required. By submitting this signed proposal I will accept a contract if approved by the City and such acceptance covers all terms, conditions, and specifications of this bid/proposal. The below signatory also hereby agrees, by virtue of submitting or attempting to submit a response, that in no event shall the City's liability for respondent's direct, indirect, incidental, consequential, special or exemplary damages, expenses, or lost profits arising out of this competitive solicitation process, including but not limited to public advertisement, bid conferences, site visits, evaluations, oral presentations, or award proceedings exceed the amount of Five Hundred Dollars ($500.00). This limitation shall not apply to claims arising under any provision of indemnification or the City's protest ordinance contained in this competitive solicitation.

Submitted by:

Josh Isner
Name (printed)

Signature

October 27, 2016
Date:

EVP, Global Sales
Title

revised 04/10/15

ADDENDUM NO. 1 through 5

RFP/ ITB No. 766-11825
TITLE: Integrated Body Worn Cameras and Digital Evidence Management System

ISSUED: 10/28/2016

This addendum is being issued to make the following change(s):

1. Bid Bond has been set to $30,000 (see section 1.3 of the RFQ).

2. Attachment-A has been modified and latest version added on 10/27/2016.

3. The opening date has been changed to 11/04/2016 at 2 P.M.

All other terms, conditions, and specifications remain unchanged.

Adam Makarevich
Procurement Specialist II

Company Name: TASER International, Inc.
(please print)

Bidder's Signature: ______________________

Date: October 28, 2016

October 24, 2016

City of Fort Lauderdale
Procurement Services Division
Room 619, City Hall
100 North Andrews Avenue
Fort Lauderdale, Florida 33301
Attn: Adam Makarevich

RE: REQUESTED EXCEPTIONS TO CITY OF FORT LAUDERDALE SOLICITATION 766-11825 FOR INTEGRATED BODY WORN CAMERAS AND DIGITAL EVIDENCE MANAGEMENT

Dear Mr. Makarevich:

Please find below TASER International, Inc.'s (TASER) exceptions to the above-referenced solicitation. TASER is open to further discussions regarding requested changes, and it reserves the right to negotiate the terms of the Terms and Conditions attached to the Solicitation.

1. **Addition of TASER's Terms and Conditions.**
TASER respectfully requests that its Master Services and Purchase Agreement be incorporated as an exhibit into the final contract award. TASER agrees to negotiate with the City on these terms and conditions, and if any of TASER's terms and conditions conflict with the negotiated terms and conditions of the contract documents, **the City's contract document will control**.

2. **Introduction to Request for Qualification. Section 1.17**
TASER respectfully requests that the second paragraph of this section be amended as follows:
The City of Fort Lauderdale shall be given notice 30~~10~~ days prior to cancellation or modification of any stipulated insurance. The insurance provided shall be endorsed or amended to comply with this notice requirement. In the event that the insurer is unable to accommodate, it shall be the responsibility of the Respondents to provide the proper notice. Such notification will be in writing by registered mail, return receipt requested and addressed to the Procurement Services Division.

3. **Scope of Services. Section 2.14(e)**
TASER respectfully requests that this section be amended as follows:
FLPD will ~~not~~ pay annual maintenance or support fees in advance of services being provided. In the event the Contract is terminated, the Successful Proposer will issue a refund of any prepaid amounts on a prorated basis. Maintenance and support should be provided to FLPD at no change for a period of one (1) year after Final Acceptance by FLPD.

4. **Special Terms and Conditions. Section 3.1.**
TASER respectfully requests that the last paragraph of this section be amended as follows:
The Successful Proposer represents and warrants to FLPD that the proposed system is free from defects and will function and perform as represented by the Successful Proposer. The Successful Proposer warrants the fitness of the proposed system to meet FLPD requirements as reflected in Successful Proposer's response to Attachment A, - Functional and Non- Functional Requirements. A breach by the Successful Proposer of this provision of the Contract, that remains uncured by the Successful Proposer for thirty days after notification from FLPD, may result in termination for cause and the Successful Proposer shall return to FLPD all amounts paid under the Contract within five business days of notification of breach by FLPD.

5. **Special Terms and Conditions. Section 3.9.**
TASER respectfully requests that this section be amended as follows:
The title and risk of loss of the hardware/software shall not pass to the City or any participating agency and any/all system parts listed herein until they actually receive~~,~~ take possession~~ and accept~~ of the goods at the point or points of delivery. In the event any hardware arrives damaged or defective, the Successful Proposer will repair or replace such hardware at no cost to the City. All products furnished hereunder shall be delivered free on board (F.O.B.) FLPD facility destination.

Best Regards,

Alissa McDowell

Alissa McDowell
Contracts Manager
amcdowell@taser.com
480.905.2038

MASTER SERVICES AND PURCHASING AGREEMENT

between

TASER INTERNATIONAL, INC.

and

Ft. Lauderdale Police Dept. - FL

CITY Agreement Number:

MASTER SERVICES AND PURCHASING AGREEMENT

This Master Agreement (the **Agreement**) by and between TASER International, Inc., (**TASER or Party**) a Delaware corporation having its principal place of business at 17800 N 85th Street, Scottsdale, Arizona, 85255, and Ft. Lauderdale Police Dept. - FL , (**Agency, Party** or collectively **Parties**) having its principal place of business at 1300 W. BROWARD BLVD, Fort Lauderdale, FL, 33312, is entered into as of December, 31, 2016 (**the Effective Date**).

This Agreement sets forth the terms and conditions for the purchase, delivery, use, and support of TASER products and services as detailed in Quote # Q-87708 (the **Quote**), which is hereby incorporated by reference. It is the intent of the Parties that this Agreement shall act as a master agreement governing all subsequent purchases by Agency of TASER Products and all subsequent quotes accepted by Agency shall be also incorporated by reference as a Quote. In consideration of this Agreement the Parties agree as follows:

1 **Term.** This Agreement will commence on the Effective Date and will remain in full force and effect until terminated by either Party. TASER services will not be authorized until a signed Quote or Purchase Order is received, whichever is first.

1.1 **Evidence.com Subscription Term:** The Initial Term of the Subscription services will begin after shipment of the Product. If shipped in 1st half of the month, the start date is on the 1st of the following month. If shipped in the last half of the month, the start date is on the 15th of the following month. Subscription Services will automatically renew for additional successive Terms of one (1) year after completion of the initial Term at the list price then in effect, unless the Agency gives TASER written notice of termination within sixty (60) days prior to the end of a one (1) year period.

1.2 **Professional Services Term:** Amounts pre-paid for professional services as outlined in the Quote and the Professional Service Appendix must be used within 6 months of the Effective Date.

2 **Definitions.**

"Business Day" means Monday through Friday, excluding holidays.

"Confidential Information" means all nonpublic information disclosed by TASER, TASER affiliates, business partners of TASER or their respective employees, contractors or agents that is designated as confidential or that, given the nature of the information or circumstances surrounding its disclosure, reasonably should be understood to be confidential.

"Documentation" means the (i) specifications, explanatory or informational materials, whether in paper or electronic form, that relate to the Services provided under this Agreement, or (ii) user manuals, technical manuals, training manuals, warnings, specification or other explanatory or informational materials, whether in paper or electronic form, that relate to the Products provided under this Agreement.

"Evidence.com Service" means TASER web services for Evidence.com, the Evidence.com site, EVIDENCE Sync software, EVIDENCE Mobile App, Axon® Mobile App, other software, maintenance, storage, and product or service provided by us under this Agreement for use with Evidence.com. This does not include any Third Party Applications, hardware warranties, or the my.evidence.com services.

"**Installation Site**" means the location(s) where the Products are to be installed.

"Policies" means the Trademark Use Guidelines, all restrictions described on the TASER website, and any other policy or terms referenced in or incorporated into this Agreement. Policies do not include whitepapers or other marketing materials.

"Products" means all TASER equipment, software, cloud based services, Documentation and software maintenance releases and updates provided by TASER under this Agreement.

"Quote" is an offer to sell, is valid only for products and services listed on the quote at prices on the quote. All Quotes referenced in this Agreement or issued and accepted after the Effective Date of this Agreement will be subject to the terms of this Agreement. Any terms and conditions contained within the Agency's purchase order in response to the Quote will be null and void and shall have no force or effect. TASER is not responsible for pricing, typographical, or other errors in any offer by TASER and TASER reserves the right to cancel any orders resulting from such errors. TASER reserves the right to adjust prices or Products unless otherwise specified in the Quote.

"Resolution Time" means the elapsed time between TASER's acknowledgment of an issue until the problem in the Services has been resolved, which does not include time delays caused by the Agency or by third parties outside of TASER's reasonable control.

"Services" means all services provided by TASER pursuant to this Agreement.

"Agency Content" means software, data, text, audio, video, images or other Agency content or any of the Agency's end users (a) run on the Evidence.com Services, (b) cause to interface with the Evidence.com Services, or (c) upload to the Evidence.com Services under the Agency account or otherwise transfer, process, use or store in connection with the Agency account.

3 **<u>Payment Terms</u>.** Invoices are due to be paid within 30 days of the date of invoice. All orders are subject to prior credit approval. Payment obligations are non-cancelable and fees paid are non-refundable and all amounts payable will be made without setoff, deduction, or withholding. If a delinquent account is sent to collections, the Agency is responsible for all collection and attorneys' fees.

4 **<u>Taxes</u>.** Unless TASER is provided with a valid and correct tax exemption certificate applicable to the purchase and ship-to location, the Agency is responsible for sales and other taxes associated with the order.

5 **<u>Shipping; Title; Risk of Loss; Rejection</u>.** TASER reserves the right to make partial shipments and products may ship from multiple locations. All shipments are E.X.W. via common carrier and title and risk of loss pass to the Agency upon delivery to the common carrier by TASER. The Agency is responsible for all freight charges. Any loss or damage that occurs during shipment is the Agency's responsibility. Shipping dates are estimates only. The Agency may reject nonconforming Product by providing TASER written notice of rejection within 10 days of shipment. Failure to notify TASER within the 10 day rejection period will be deemed as acceptance of Product.

6 **Returns.** All sales are final and no refunds or exchanges are allowed, except for warranty returns or as provided by state or federal law.

7 **Warranties.**

7.1 **Hardware Limited Warranty.** TASER warrants that its law enforcement hardware products are free from defects in workmanship and materials for a period of ONE (1) YEAR from the date of receipt. Extended warranties run from the date of purchase of the extended warranty through the balance of the 1-year limited warranty term plus the term of the extended warranty measured after the expiration of the 1-year limited warranty. CEW cartridges and Smart cartridges that are expended are deemed to have operated properly. TASER-Manufactured Accessories are covered under a limited 90-DAY warranty from the date of receipt. Non-TASER manufactured accessories are covered under the manufacturer's warranty. If TASER determines that a valid warranty claim is received within the warranty period, TASER agrees to repair or replace the Product. TASER's sole responsibility under this warranty is to either repair or replace with the same or like Product, at TASER's option.

7.2 **Warranty Limitations.**

7.2.1 The warranties do not apply and TASER will not be responsible for any loss, data loss, damage, or other liabilities arising from: (a) damage from failure to follow instructions relating to the Product's use; (b) damage caused by use with non-TASER products or from the use of cartridges, batteries or other parts, components or accessories that are not manufactured or recommended by TASER; (c) damage caused by abuse, misuse, intentional or deliberate damage to the product, or force majeure; (d) damage to a Product or part that has been repaired or modified by persons other than TASER authorized personnel or without the written permission of TASER; or (e) if any TASER serial number has been removed or defaced.

7.2.2 **To the extent permitted by law, the warranties and the remedies set forth above are exclusive and TASER disclaims all other warranties, remedies, and conditions, whether oral or written, statutory, or implied, as permitted by applicable law. If statutory or implied warranties cannot be lawfully disclaimed, then all such warranties are limited to the duration of the express warranty described above and limited by the other provisions contained in this Agreement.**

7.2.3 **TASER's cumulative liability to any Party for any loss or damage resulting from any claims, demands, or actions arising out of or relating to any TASER product will not exceed the purchase price paid to TASER for the product or if for services, the amount paid for such services over the prior 12 months preceding the claim. In no event will either Party be liable for any direct, special, indirect, incidental, exemplary, punitive or consequential damages, however caused, whether for breach of warranty, breach of contract, negligence, strict liability, tort or under any other legal theory**.

7.3 **Warranty Returns.** If a valid warranty claim is received by TASER within the warranty period, TASER agrees to repair or replace the Product which TASER determines in its sole discretion to be defective under normal use, as defined in the Product instructions. TASER's sole responsibility under this warranty is to either repair or replace with the same or like Product, at TASER's option.

7.3.1 For warranty return and repair procedures, including troubleshooting guides, please go to TASER's websites www.taser.com/support or www.evidence.com, as indicated in the appropriate product user manual or quick start guide.

7.3.2 Before delivering product for warranty service, it is the Agency's responsibility to upload the data contained in the product to the EVIDENCE.com services or download the product data and keep a separate backup copy of the contents. TASER is not responsible for any loss of software programs, data, or other information contained on the storage media or any other part of the product services.

7.3.3 A replacement product will be new or like new and have the remaining warranty period of the original product or 90 days from the date of replacement or repair, whichever period is longer. When a product or part is exchanged, any replacement item becomes Purchaser's property and the replaced item becomes TASER's property.

8 **Product Warnings.** See our website at www.TASER.com for the most current product warnings.

9 **Design Changes.** TASER reserves the right to make changes in the design of any of TASER's products and services without incurring any obligation to notify the Agency or to make the same change to products and services previously purchased.

10 **Insurance.** TASER will maintain at TASER's own expense and in effect during the Term, Commercial General Liability Insurance, Workers' Compensation Insurance and Commercial Automobile Insurance and will furnish certificates of insurance or self-insurance upon request.

11 **Indemnification.** TASER will indemnify and defend the Agency Indemnitees (the Agency's officers, directors, and employees) from and against all claims, demands, losses, liabilities, reasonable costs and expenses arising out of a claim by a third party against an Agency Indemnitee resulting from any negligent act, error or omission, or willful misconduct of TASER under or related to this Agreement, except in the case of negligent acts, omissions or willful misconduct of the Agency or claims that fall under Workers Compensation coverage.

12 **IP Rights.** TASER owns and reserves all right, title, and interest in the TASER Products and related software, as well as any suggestions made to TASER.

13 **IP Indemnification.** TASER will defend, indemnify, and hold the Agency Indemnitees harmless from and against any claims, damages, losses, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or relating to any third-party claim alleging that use of TASER Products or Services as permitted under this Agreement infringes or misappropriates the intellectual property rights of a third party. The Agency must provide TASER with prompt written notice of such a claim, tender to us the defense or settlement of such a claim at our expense, and cooperate fully with us in the defense or settlement of such a claim.

TASER has no liability to the Agency or any third party if any alleged infringement or claim of infringement is to any extent based upon: (a) any modification of the Evidence.com Services by the

Agency or any third party not approved by TASER; (b) use of the Evidence.com Services in connection or in combination with equipment, devices, or services not approved or recommended by TASER; (c) the use of Evidence.com Services other than as permitted under this Agreement or in a manner for which it was not intended; or (d) the use of other than the most current release or version of any software provided by TASER as part of or in connection with the Evidence.com Services. Nothing in this Section will affect any warranties in favor of the Agency that are otherwise provided in or arise out of this Agreement.

14 **Agency Responsibilities.** The Agency is responsible for (i) use of TASER Products (including any activities under the Agency Evidence.com account and use by Agency employees and agents), (ii) breach of this Agreement or violation of applicable law by the Agency or any of the Agency's end users, (iii) Agency Content or the combination of Agency Content with other applications, content or processes, including any claim involving alleged infringement or misappropriation of third party rights by Agency Content or by the use of Agency Content, (iv) a dispute between the Agency and any third party over Agency use of TASER products or the collection or use of Agency Content, (v) any hardware or networks that the Agency connects to the Evidence.com Services, and (vi) any security settings the Agency establishes to interact with or on the Evidence.com Services.

15 **Termination.**

15.1 By Either Party. Either Party may terminate for cause upon 30 days advance notice to the other Party if there is any material default or breach of this Agreement by the other Party, unless the defaulting Party has cured the material default or breach within the 30-day notice period. In the event that the Agency terminates this Agreement under this Section and TASER fails to cure the material breach or default, TASER will issue a refund of any prepaid amounts on a prorated basis.

15.2 By Agency. The Agency is obligated to pay the fees under this Agreement as may lawfully be made from funds budgeted and appropriated for that purpose during the then current fiscal year. In the event that sufficient funds will not be appropriated or are not otherwise legally available to pay the fees required under this Agreement, this Agreement may be terminated by the Agency. The Agency agrees to deliver notice of termination under this Section at least 90 days prior to the end of the then current fiscal year.

15.3 Effect of Termination. Upon any termination of this Agreement: (a) all Agency rights under this Agreement immediately terminate; (b) the Agency remains responsible for all fees and charges incurred through the date of termination; and (c) Payment Terms, Warranty, Product Warnings, Indemnification, and Agency Responsibilities Sections, as well as the Evidence.com Terms of Use Appendix Sections on Agency Owns Agency Content, Data Storage, Fees and Payment, Software Services Warranty, IP Rights and License Restrictions will continue to apply in accordance with their terms.

15.4 After Termination. TASER will not delete any Agency Content as a result of a termination during a period of 90 days following termination. During this 90-day period the Agency may retrieve Agency Content only if all amounts due have been paid (there will be no application functionality of the Evidence.com Services during this 90-day period other than the ability to retrieve Agency Content). The Agency will not incur any additional fees if Agency Content is downloaded from Evidence.com during this 90-day period. TASER has no obligation to maintain or provide any Agency Content after this 90-day period and will thereafter, unless legally prohibited, delete all of Agency Content stored in the Evidence.com Services. Upon request, TASER will provide written proof that all Agency Content has been successfully deleted and fully removed from the Evidence.com Services.

15.5 **Post-Termination Assistance.** TASER will provide Agency with the same post-termination data retrieval assistance that TASER generally makes available to all customers. Requests for TASER to provide additional assistance in downloading or transferring Agency Content will result in additional fees and TASER will not warrant or guarantee data integrity or readability in the external system.

16 **General.**

16.1 **Confidentiality**. Both Parties will take all reasonable measures to avoid disclosure, dissemination or unauthorized use of either Party's Confidential Information. Except as required by applicable law, neither Party will disclose either Party's Confidential Information during the Term or at any time during the 5-year period following the end of the Term. All TASER Pricing is considered confidential and competition sensitive.

16.2 **Excusable delays**. TASER will use commercially reasonable efforts to deliver all products and services ordered as soon as reasonably practicable. In the event of interruption of any delivery due to causes beyond TASER's reasonable control TASER has the right to delay or terminate the delivery with reasonable notice.

16.3 **Force Majeure**. Neither Party will be liable for any delay or failure to perform any obligation under this Agreement where the delay or failure results from any cause beyond the Parties' reasonable control, including acts of God, labor disputes or other industrial disturbances, systemic electrical, telecommunications, or other utility failures, earthquake, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism, or war.

16.4 **Proprietary Information**. The Agency agrees that TASER has and claims various proprietary rights in the hardware, firmware, software, and the integration of ancillary materials, knowledge, and designs that constitute TASER products and services, and that the Agency will not directly or indirectly cause any proprietary rights to be violated.

16.5 **Independent Contractors**. The Parties are independent contractors. Neither Party, nor any of their respective affiliates, has the authority to bind the other. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary, or employment relationship between the Parties.

16.6 **No Third Party Beneficiaries**. This Agreement does not create any third party beneficiary rights in any individual or entity that is not a party to this Agreement.

16.7 **Non-discrimination and Equal Opportunity**. During the performance of this Agreement, neither the Parties nor the Party's employees will discriminate against any person, whether employed by a Party or otherwise, on the basis of basis of race, color, religion, gender, age, national origin, handicap, marital status, or political affiliation or belief. In all solicitations or advertisements for employees, agents, subcontractors or others to be engaged by a Party or placed by or on behalf of a Party, the solicitation or advertisement shall state all qualified applicants shall receive consideration for employment without regard to race, color, religion, gender, age, national origin, handicap, marital status, or political affiliation or belief.

16.8 **U.S. Government Rights**. Any Evidence.com Services provided to the U.S. Government as "commercial items," "commercial computer software," "commercial computer software documentation," and "technical data" will have the same rights and restrictions generally applicable to the Evidence.com Services. If the Agency is using the Evidence.com Services on behalf of the U.S. Government and these terms fail to meet the U.S. Government's needs or are inconsistent in any respect with federal law, the Agency will immediately discontinue use of the Evidence.com Services. The terms "commercial item," "commercial computer software," "commercial computer software documentation," and "technical data" are defined in the Federal Acquisition Regulation and the Defense Federal Acquisition Regulation Supplement.

16.9 **Import and Export Compliance**. In connection with this Agreement, each Party will comply with all applicable import, re- import, export, and re-export control laws and regulations.

16.10 **Assignment**. Neither Party may assign or otherwise transfer this Agreement without the prior written approval of the other Party. TASER may assign or otherwise transfer this Agreement or any of our rights or obligations under this Agreement without consent (a) for financing purposes, (b) in connection with a merger, acquisition or sale of all or substantially all of our assets, (c) as part of a corporate reorganization, or (d) to a subsidiary corporation. Subject to the foregoing, this Agreement will be binding upon the Parties and their respective successors and assigns.

16.11 **No Waivers**. The failure by either Party to enforce any provision of this Agreement will not constitute a present or future waiver of the provision nor limit the Party's right to enforce the provision at a later time.

16.12 **Severability**. This Agreement is contractual and not a mere recital. If any portion of this Agreement is held to be invalid or unenforceable, the remaining portions of this Agreement will remain in full force and effect.

16.13 **Governing Law; Venue**. The laws of the state where the Agency is physically located, without reference to conflict of law rules, govern this Agreement and any dispute of any sort that might arise between the Parties. The United Nations Convention for the International Sale of Goods does not apply to this Agreement.

16.14 **Notices**. All communications and notices to be made or given pursuant to this Agreement must be in the English language. Notices provided by posting on the Agency's Evidence.com site will be effective upon posting and notices provided by email will be effective when the email was sent. Notices provided by personal delivery will be effective immediately. Contact information for notices:

TASER: TASER International, Inc.
ATTN: Contracts
17800 N. 85th Street
Scottsdale, Arizona 85255
contracts@taser.com

AGENCY:

16.15 Entire Agreement. This Agreement, including the APPENDICES attached hereto, and the Policies and the quote provided by TASER, represents the entire agreement between the Parties. This Agreement supersedes all prior or contemporaneous representations, understandings, agreements, or communications between the Parties, whether written or verbal, regarding the subject matter of this Agreement. No modification or amendment of any portion of this Agreement will be effective unless in writing and signed by the Parties to this Agreement. If TASER provides a translation of the English language version of this Agreement, the English language version of the Agreement will control if there is any conflict.

16.16 Counterparts. If this Agreement form requires the signatures of the Parties, then this Agreement may be executed by electronic signature in multiple counterparts, each of which is considered an original.

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement to be duly executed. Each Party warrants and represents that its respective signatories whose signatures appear below have been and are, on the date of signature, duly authorized to execute this Agreement.

TASER International, Inc.
Signature: ______________________________
Name: __________________________
Title: ______________________________
Date: ______________________________
Address: 17800 N. 85th Street Scottsdale, AZ 85255

Attn: Contracts

Email: contracts@taser.com

Ft. Lauderdale Police Dept. - FL
Signature: ______________________________
Name: __________________________
Title: ______________________________
Date: ______________________________
Address: 1300 W. BROWARD BLVD, Fort Lauderdale, FL, 33312

Evidence.com Terms of Use
Appendix

1 **<u>Access Rights</u>.** Upon the purchase or granting of a subscription from TASER and the opening of an Evidence.com account the Agency will have access and use of the Evidence.com Services for the storage and management of Agency Content during the subscription term (**Term**). The Evidence.com Service and data storage are subject to usage limits. The Evidence.com Service may not be accessed by more than the number of end users specified in the Quote. If Agency becomes aware of any violation of this Agreement by an end user, the Agency will immediately terminate that end user's access to Agency Content and the Evidence.com Services.

2 **<u>Agency Owns Agency Content</u>.** The Agency controls and owns all right, title, and interest in and to Agency Content and TASER obtains no rights to the Agency Content and the Agency Content are not business records of TASER. The Agency is solely responsible for the uploading, sharing, withdrawal, management and deletion of Agency Content. TASER will have limited access to Agency Content solely for the purpose of providing and supporting the Evidence.com Services to the Agency and Agency end users. The Agency represents that the Agency owns Agency Content; and that none of Agency Content or Agency end users' use of Agency Content or the Evidence.com Services will violate this Agreement or applicable laws.

3 **<u>Evidence.com Data Security</u>.**

3.1. Generally. TASER will implement commercially reasonable and appropriate measures designed to secure Agency Content against accidental or unlawful loss, access or disclosure. TASER will maintain a comprehensive Information Security Program (**ISP**) that includes logical and physical access management, vulnerability management, configuration management, incident monitoring and response, encryption of digital evidence uploaded, security education, risk management, and data protection. The Agency is responsible for maintaining the security of end user names and passwords and taking steps to maintain appropriate security and access by end users to Agency Content. Log-in credentials are for Agency internal use only and Agency may not sell, transfer, or sublicense them to any other entity or person. The Agency agrees to be responsible for all activities undertaken by the Agency, Agency employees, Agency contractors or agents, and Agency end users which result in unauthorized access to the Agency account or Agency Content. Audit log tracking for the video data is an automatic feature of the Services which provides details as to who accesses the video data and may be downloaded by the Agency at any time. The Agency shall contact TASER immediately if an unauthorized third party may be using the Agency account or Agency Content or if account information is lost or stolen.

3.2. FBI CJIS Security Addendum. For customers based in the United States, TASER agrees to the terms and requirements set forth in the Federal Bureau of Investigation (**FBI**) Criminal Justice Information Services (**CJIS**) Security Addendum for the Term of this Agreement.

4 **<u>Our Support</u>.** TASER will make available updates as released by TASER to the Evidence.com Services. Updates may be provided electronically via the Internet. TASER will use reasonable efforts to continue supporting the previous version of any API or software for 6 months after the change (except if doing so (a) would pose a security or intellectual property issue, (b) is economically or technically

burdensome, or (c) is needed to comply with the law or requests of governmental entities. The Agency is responsible for maintaining the computer equipment and Internet connections necessary for use of the Evidence.com Services.

5 **Data Privacy.** TASER will not disclose Agency Content or any information about the Agency except as compelled by a court or administrative body or required by any law or regulation. TASER will give notice if any disclosure request is received for Agency Content so the Agency may file an objection with the court or administrative body. The Agency agrees to allow TASER access to certain information from the Agency in order to: (a) perform troubleshooting services for the account upon request or as part of our regular diagnostic screenings; (b) enforce this agreement or policies governing use of Evidence.com Services; or (c) perform analytic and diagnostic evaluations of the systems.

6 **Data Storage.** TASER will determine the locations of the data centers in which Agency Content will be stored and accessible by Agency end users. For United States customers, TASER will ensure that all Agency Content stored in the Evidence.com Services remains within the United States including any backup data, replication sites, and disaster recovery sites. TASER may transfer Agency Content to third parties for the purpose of storage of Agency Content. Third party subcontractors responsible for storage of Agency Content are contracted by TASER for data storage services. Ownership of Agency Content remains with the Agency. For use of an Unlimited Evidence.com License unlimited data may be stored in the Agency's Evidence.com account if the data originates from a TASER device. For use of Totally Unlimited Evidence.com Licenses TASER reserves the right to limit the types of content the Agency can store and share using the Services.

7 **Fees and Payment.** Additional end users may be added during the Term at the pricing in effect at the time of purchase of additional end users, prorated for the duration of the Term. Additional end user accounts will terminate on the same date as the pre-existing subscriptions. TASER reserves the right to charge additional fees for exceeding purchased storage amounts or for TASER's assistance in the downloading or exporting of Agency Content.

8 **Suspension of Evidence.com Services.** TASER may suspend Agency access or any end user's right to access or use any portion or all of the Evidence.com Services immediately upon notice in accordance with the following:

8.1. The Termination provisions of the Master Service Agreement apply;

8.2. The Agency or an end user's use of or registration for the Evidence.com Services (i) poses a security risk to the Evidence.com Services or any third party, (ii) may adversely impact the Evidence.com Services or the systems or content of any other customer, (iii) may subject TASER, TASER's affiliates, or any third party to liability, or (iv) may be fraudulent;

8.3. If TASER suspends the right to access or use any portion or all of the Evidence.com Services, the Agency remains responsible for all fees and charges incurred through the date of suspension without any credits for any period of suspension. TASER will not delete any of Agency Content on Evidence.com as a result of a suspension, except as specified elsewhere in this Agreement.

9 **Software Services Warranty**. TASER warrants that the Evidence.com Services will not infringe or misappropriate any patent, copyright, trademark, or trade secret rights of any third party. TASER disclaims any warranties or responsibility for data corruption or errors before the data is uploaded to the Evidence.com Services.

10 **License Restrictions**. Neither the Agency nor any Agency end users may, or attempt to: (a) permit any third party to access the Evidence.com Services except as permitted in this Agreement; (b) modify, alter, tamper with, repair, or otherwise create derivative works of any of the Evidence.com Services; (c) reverse engineer, disassemble, or decompile the Evidence.com Services or apply any other process or procedure to derive the source code of any software included in the Evidence.com Services, or allow any others to do the same; (d) access or use the Evidence.com Services in a way intended to gain unauthorized access, avoid incurring fees or exceeding usage limits or quotas; (e) copy the Evidence.com Services in whole or part, except as expressly permitted in this Agreement; (f) use trade secret information contained in the Evidence.com Services, except as expressly permitted in this Agreement; (g) resell, rent, loan, or sublicense the Evidence.com Services; (h) access the Evidence.com Services in order to build a competitive product or service or copy any features, functions, or graphics of the Evidence.com Services; (i) remove, alter, or obscure any confidentiality or proprietary rights notices (including copyright and trademark notices) of ours or our licensors on or within the Evidence.com Services or any copies of the Evidence.com Services; or (j) use the Evidence.com Services to store or transmit infringing, libelous, or otherwise unlawful or tortious material, to store or transmit material in violation of third party privacy rights, or to store or transmit malicious code. All licenses granted in this Agreement are conditional on continued compliance this Agreement, and will immediately and automatically terminate if the Agency does not comply with any term or condition of this Agreement. The Agency may only use our trademarks in accordance with the TASER Trademark Use Guidelines (located at www.TASER.com).

Professional Services
Appendix

1 **Scope of Services.** The project scope will consist of the Services identified on the Quote.

1.1. The Package for the Axon and Evidence.com related Services are detailed below:

System set up and configuration Setup Axon® Mobile on smart phones (if applicable). Configure categories & custom roles based on Agency need. Troubleshoot IT issues with Evidence.com and Evidence.com Dock (Dock) access. Work with IT to install EVIDENCE Sync software on locked-down computers (if applicable). One on-site session Included
Dock installation Work with Agency to decide ideal location of Dock setup and set configurations on Dock if necessary. Authenticate Dock with Evidence.com using "admin" credentials from Agency. Work with Agency's IT to configure its network to allow for maximum bandwidth and proper operation within Agency's network environment. On site Assistance Included
Dedicated Project Manager Assignment of a specific TASER representative for all aspects of planning the Product rollout (Project Manager). Ideally, the Project Manager will be assigned to the Agency 4–6 weeks prior to rollout.
Weekly project planning meetings Project Manager will develop a Microsoft Project plan for the rollout of Axon camera units, Docks and Evidence.com account training based on size, timing of rollout and Agency's desired level of training. Up to 4 weekly meetings leading up to the Evidence.com Dock installation of not more than 30 minutes in length.
Best practice implementation planning session—1 on-site session to: Provide considerations for establishment of video policy and system operations best practices based on TASER's observations with other agencies. Discuss importance of entering metadata in the field for organization purposes and other best practice for digital data management. Provide referrals of other agencies using the Axon camera products and Evidence.com services Create project plan for larger deployments. Recommend rollout plan based on review of shift schedules.
System Admin and troubleshooting training sessions 2 on-site sessions—each providing a step-by-step explanation and assistance for Agency's configuration of security, roles & permissions, categories & retention, and other specific settings for Evidence.com.
Axon instructor training Prior to general user training on Axon camera systems and Evidence.com services, TASER's on-site professional services team will provide training for instructors who can support the Agency's subsequent Axon camera and Evidence.com training needs.
End user go live training and support sessions Provide individual device set up and configuration assistance; pairing with viewers when applicable; and training on device use, Evidence.com and EVIDENCE Sync.
Implementation document packet Evidence.com administrator guides, camera implementation guides, network setup guide, sample policies, and categories & roles guide

Post go live review session

1.2. Additional training days may be added on to any service package for additional fees set forth in the Quote.

2 **Out of Scope Services.** TASER is responsible to perform only the Services described on the Quote. Any additional services discussed or implied that are not defined explicitly by the Quote will be considered out of the scope.

3 **Delivery of Services.**

3.1. **Hours and Travel.** TASER personnel will work within normal business hours, Monday through Friday, 8:30 a.m. to 5:30 p.m., except holidays unless otherwise agreed in advance. All tasks on-site will be performed over a consecutive timeframe unless otherwise agreed to by the Parties in advance. Travel time by TASER personnel to Agency premises will not be charged as work hours performed.

3.2. **Changes to Services.** Changes to the scope of Services must be documented and agreed upon by the Parties in a change order. Changes may require an equitable adjustment in the charges or schedule.

4 **Authorization to Access Computer Systems to Perform Services.** The Agency authorizes TASER to access relevant Agency computers and network systems solely for the purpose of performing the Services. TASER will work diligently to identify as soon as reasonably practicable the resources and information TASER expects to use, and will provide an initial itemized list to the Agency. The Agency is responsible for, and assumes the risk of any problems, delays, losses, claims, or expenses resulting from the content, accuracy, completeness, and consistency of all data, materials, and information supplied by the Agency.

5 **Site Preparation and Installation.** Prior to delivering any Services, TASER will provide 1 copy of the then-current user documentation for the Services and related Products in paper or electronic form (**Product User Documentation**). The Product User Documentation will include all environmental specifications that must be met in order for the Services and related Products to operate in accordance with the Product User Documentation. Prior to the installation of Product (whether performed by the Agency or TASER), the Agency must prepare the Installation Site in accordance with the environmental specifications set forth in the Product User Documentation. Following the installation of the Products, the Agency must maintain the Installation Site where the Products have been installed in accordance with the environmental specifications set forth in the Product User Documentation. In the event that there are any updates or modifications to the Product User Documentation for any Products provided by TASER under this Agreement, including the environmental specifications for the Products, TASER will provide the updates or modifications to Agency when they are generally released by TASER to TASER customers.

6 **Acceptance Checklist.** TASER will present an Acceptance Checklist (**Checklist**) upon completion of

the Services that will exactly mirror the description of services within this Section. The Agency will sign the Checklist acknowledging completion of the Services once the on-site service session has been completed. If the Agency reasonably believes that TASER did not complete the Services in substantial conformance with this Agreement, the Agency must notify TASER in writing of the specific reasons for rejection of the Services within 7 calendar days from delivery of the Checklist. TASER will address the issues and then will re-present the Checklist for approval and signature. If TASER does not receive the signed Checklist or a written notification of the reasons for the rejection of the performance of the Services within 7 calendar days of delivery of the Checklist, the absence of the Agency response will constitute affirmative acceptance of the Services, and a waiver of any right of rejection.

7 **Liability for Loss or Corruption of Data.** The Agency is responsible for: (i) instituting proper and timely backup procedures for Agency software and data; (ii) creating timely backup copies of Agency software or data that may be damaged, lost, or corrupted due to our provision of Services; and (iii) using backup copies to restore any Agency software or data in the event of any loss of, damage to, or corruption of the operational version of Agency software or data, even if such damage, loss, or corruption is due to TASER negligence. However, regardless of any assistance provided by TASER: (i) TASER will in no way be liable for the accuracy, completeness, success, or results of efforts to restore Agency software or data; (ii) any assistance provided by TASER under this Section is without warranty, express or implied; and (iii) in no event will TASER be liable for loss of, damage to, or corruption of Agency data from any cause.

TASER Assurance Plan
Appendix

The TASER Assurance Plan or "TAP" has been purchased as part of the Quote attached to this Agreement. TAP provides hardware extended warranty coverage, Spare Products, and Upgrade Models at the end of the TAP Term. TAP only applies to the TASER Product listed in the Quote with the exception of any initial hardware or any software services offered for, by, or through the Evidence.com website. The Agency may not buy more than one TAP for any one covered Product.

1 **TAP Warranty Coverage**. TAP includes the extended warranty coverage described in the current hardware warranty. TAP warranty coverage starts at the beginning of the TAP Term and continues as long as the Agency continues to pay the required annual fees for TAP. The Agency may not have both an optional extended warranty and TAP on the Axon camera/Dock product. TAP for the Axon camera products also includes free replacement of the Axon flex controller battery and Axon body battery during the TAP Term for any failure that is not specifically excluded from the Hardware Warranty.

2 **TAP Term**. TAP Term start date is based upon the shipment date of the hardware covered under TAP. If the shipment of the hardware occurred in the first half of the month, then the Term starts on the 1st of the following month. If the shipment of the hardware occurred in the second half of the month, then the Term starts on the 15th of the following month.

3 **SPARE Product**. TASER will provide a predetermined number of spare Products for those hardware items and accessories listed in the Quote (collectively the "Spare Products") to keep at the Agency location to replace broken or non-functioning units in order to improve the availability of the units to officers in the field. The Agency must return to TASER, through TASER's RMA process, any broken or non-functioning units for which a Spare Product is utilized, and TASER will repair or replace the non-functioning unit with a replacement product. TASER warrants it will repair or replace the unit which fails to function for any reason not excluded by the TAP warranty coverage, during the TAP Term with the same product or a like product, at TASER's sole option. The Agency may not buy a new TAP for the replacement product or the Spare Product.

3.1. Within 30 days of the end of the TAP Term the Agency must return to TASER all Spare Products. The Agency will be invoiced for and are obligated to pay to TASER the MSRP then in effect for all Spare Products not returned to TASER. If all the Spare Products are returned to TASER, then TASER will refresh the allotted number of Spare Products with Upgrade Models if the Agency purchases a new TAP for the Upgrade Models.

4 **TAP Upgrade Models**. Upgrade Models are to be provided as follows during and/or after the TAP Term: (i) an upgrade will provided in year 3 if the Agency purchased 3 years of Evidence.com services with Ultimate Licenses or Unlimited Licenses and all TAP payments are made; or (ii) 2.5 years after the Effective Date and once again 5 years after the Effective Date if the Agency purchased 5 years of Evidence.com services with an Ultimate License or Unlimited Licenses or OSP and made all TAP payments.

Any products replaced within the six months prior to the scheduled upgrade will be deemed the Upgrade Model. Thirty days after the Upgrade Models are received, the Agency must return the products to TASER or TASER will deactivate the serial numbers for the products received unless the Agency purchases additional Evidence.com licenses for the Axon camera products the Agency is keeping. The Agency may buy a new TAP for any Upgraded Model.

4.1. **TAP Axon Camera Upgrade Models**.

4.1.1. If the Agency purchased TAP for Axon Cameras as a stand-alone service, then TASER will upgrade the Axon camera (and controller if applicable), free of charge, with a new on-officer video camera that is the same product or a like product, at TASER's sole option. TASER makes no guarantee that the Upgrade Model will utilize the same accessories or Dock. If the Agency would like to change product models for the Upgrade Model, then the Agency must pay the price difference in effect at the time of the upgrade between the MSRP for the offered Upgrade Model and the MSRP for the model that will be acquired. No refund will be provided if the MSRP of the new model is less than the MSRP of the offered Upgrade Model.

4.1.2. If the Agency purchased Unlimited License or OSP, then TASER will upgrade the Axon camera (and controller if applicable), free of charge, with a new on-officer video camera of the Agency's choice.

4.2. **TAP Dock Upgrade Models**. TASER will upgrade the Dock free of charge, with a new Dock with the same number of bays that is the same product or a like product, at TASER's sole option. If the Agency would like to change product models for the Upgrade Model or add additional bays, then the Agency must pay the price difference in effect at the time of the upgrade between the MSRP for the offered Upgrade Model and the MSRP for the model desired. No refund will be provided if the MSRP of the new model is less than the MSRP of the offered Upgrade Model.

5 **<u>TAP Termination</u>.** If an invoice for TAP is more than 30 days past due or the Agency defaults on its payments for the Evidence.com services then TASER may terminate TAP and all outstanding Product related TAPs. TASER will provide notification that TAP coverage is terminated. Once TAP coverage is terminated for any reason, then:

5.1. TAP coverage will terminate as of the date of termination and no refunds will be given.

5.2. TASER will not and has no obligation to provide the free Upgrade Models.

5.3. The Agency will be invoiced for and are obligated to pay to TASER the MSRP then in effect for all Spare Products provided under TAP. If the Spare Products are returned within 30 days of the Spare Product invoice date, credit will be issued and applied against the Spare Product invoice.

5.4. The Agency will be responsible for payment of any missed payments due to the termination before being allowed to purchase any future TAP.

5.5. If the Agency received Axon Products free of charge and TAP is terminated before the end of the term then (a) the Agency will be invoiced for the remainder of the MSRP for the Products received and not already paid as part of the TAP before the termination date; or (b) only in the case of termination for non-appropriations, return the Products to TASER within 30 days of the date of termination.

Service Level Agreement
Appendix

This Service Level Agreement (**SLA**) is a policy governing the use of the Evidence.com™ Service offerings.

1 **Service Commitment**. Apart from maintenance described in Section 2, TASER will use reasonable efforts to make the Service Offerings available 99.9% of the time 7 days per week on a 24-hour basis.

2 **Maintenance**.

2.1 Scheduled maintenance will take place according to our prevailing routine maintenance schedule. Routine maintenance is currently scheduled on the fourth Tuesday of each month from 7:00 am to 8:00 pm Pacific Standard Time. Maintenance periods may periodically result in the Service Offerings being unavailable. When possible, TASER will give notice 1 week prior to any changes to the maintenance schedule.

2.2 Emergency maintenance may have less than a 24-hour notification period. Emergency maintenance may be performed at any time, with or without notice as deemed necessary by TASER.

3 **After Hours Emergency Support**. Evidence.com Help Desk are available at Help@EVIDENCE.com.

4 **Response Times**.

Issue Classification	Description	Targeted Response Time	Targeted Resolution Time*
Severity 1	• Business critical function is down • Material impact to Customer's business • No workaround exists	As soon as possible, using reasonable commercial efforts	Less than 24 hours
Severity 2	• Business critical function is impaired or degraded • There are time-sensitive issues that materially impact ongoing production • Workaround exists, but it is only temporary	1 Business Day	Less than 2 weeks
Severity 3	• Non-critical function down or impaired • Does not have significant current production impact • Performance is degraded	1 Business Day	Mutually agreed timeframe based on prioritization.

* Resolution time is a target, but may not be possible with all reported issues depending on circumstances.

5 **Backup**. TASER will administer system backup according to our prevailing backup plan. The Agency retains rights to all Agency Content and user data contained in the backups in

accordance with this Agreement. The Service Offerings will alert the Agency Administrator(s) of upcoming scheduled evidence deletions within the system and the Agency Administrator(s) may delay deletion by either re-categorizing that evidence or by selecting the option to extend the retention period. Once evidence is deleted it is unrecoverable.

6 **Exclusions**. The Service Commitment does not apply to any unavailability, suspension or termination of the Service Offerings, or any other Evidence.com performance issues: (a) caused by factors outside of our reasonable control, including any force majeure event, terrorism, sabotage, virus attacks, or Internet access or related problems beyond the demarcation point of the Service Offerings (including Domain Name Server issues outside TASER's direct control); (b) that result from any actions or inactions of the Agency or any third party; (c) that result from the Agency's communication delays, including wrong, bad or missing data, improperly formatted, organized or transmitted data received, or any other data issues related to the communication or data received from or through the Agency; (d) that result from Agency equipment, software or other technology and/or third party equipment, software or other technology (other than third party equipment within TASER's direct control); (e) that result from any maintenance as provided for pursuant to this SLA; or (f) arising from TASER's suspension and termination of Agency's right to use the Service Offerings in accordance with this Agreement.

[DATE]

[FIRM ADDRESS]

RE: Engagement for Expert Services

Dear [FIRM]:

This letter confirms our agreement that _______________ ("Firm") has retained TASER International, Inc., and Bryan Chiles (collectively "Expert") to serve as an expert in connection with Firm's representation of _______ ("Client") in the [TITLE OF ACTION], pending in [COURT], (the "Litigation")/[DISPUTE DISCRIPTION] (the "Matter"). The purpose of this retainer agreement ("Agreement") is to outline the nature of the engagement and the parties' responsibilities and expectations under this Agreement.

<u>Scope of Engagement</u>: Expert will provide expert witness services which may include: consulting; review of case documentation and additional research; preparation of expert reports; download analysis; full analysis; testimony at deposition and court proceedings. Expert agrees not to contact any represented parties other than through legal counsel.

<u>Confidentiality</u>: The Expert understands, agrees and accepts that it will be bound to maintain the confidences of the Client, as well as maintain the confidentiality of work product generated or compiled by Expert or Firm, under the terms and provisions which control the attorney-client privilege, the attorney work product protection, and all other applicable privileges of confidentiality which the Client or the Firm may hold under applicable federal or state law. Expert further agrees not to disclose any information, nor otherwise communicate, in any manner with any press, news, or entertainment media regarding the [LITIGATION/MATTER]. Expert further agrees to maintain the confidentiality of privileged and/or confidential records and information produced to Expert by the Firm and/or by the Client in relation to the [LITIGATION/MATTER].

Expert will promptly notify [FIRM] upon receiving a subpoena or any other official request seeking the production of documents, records or other information related to the engagement.

Expert agrees to return to the Firm all confidential information and/or all evidence, documents or materials provided to the Expert by the Firm or Client within ten (10) days of the Firm or Client's written request.

<u>Compensation and Billing</u>. Expert's hourly/fixed billing fees/rates and travel expenses are outlined in Exhibit A to this Agreement. Client agrees to pay Expert for services performed by Expert at the aforementioned rates and to pay Expert by check made payable to TASER International, Inc. Expert will submit monthly invoices to Firm for all services performed by Expert. Payment will be due within 30 days of the invoice date. Expert understands and agrees that Client is solely responsible for the payment of all fees and expenses and Firm has no liability for any portion of Expert's fees or expenses or any unpaid or disputed amounts.

<u>Conflicts of Interest</u>. Expert represents that TASER International, Inc. and Bryan Chiles have conducted a conflict of interest analysis and determined that no conflict exists that would impair Expert's ability to serve as an expert in this [LITIGATION/MATTER]. Expert agrees not to undertake during the course of

Expert's engagement with Client on the [LITIGATION/MATTER] any other engagement related to the [LITIGATION/MATTER] without the advance written consent of the Firm. Expert agrees to promptly notify the Firm if any conflict of interest should arise.

Compliance with Laws. Expert understands and agrees that all of Expert's services must be performed in compliance with all applicable laws, regulations and standards of professional conduct. Neither the Client, nor the Firm, authorizes, requires, requests, suggests, desires, or otherwise implies or permits that Expert should in any way violate or deviate from any applicable legal or ethical standard in performance of Expert's services in the [LITIGATION/MATTER].

Term and Termination. This Agreement will continue until the conclusion of Expert's services or until terminated by either party. Either party may terminate this Agreement for any reason upon 5 days written notice. Client will pay all outstanding balances within 30 days of any termination of this Agreement.

General Provisions. Both parties agree that this Agreement and all disputes arising hereunder will be governed by the laws of the State of Arizona without reference to conflict of laws principles. This Agreement constitutes the complete agreement of the parties on the subject matter covered herein and supersedes all prior or contemporaneous understandings, agreements, or representations, written or oral, of the parties. No waiver by any party of any of the provisions hereof shall be effective unless explicitly set forth in writing and signed by the party so waiving. This Agreement may not be amended except by a writing signed by both parties and expressly declared to be an amendment or modification of this Agreement. In the event that any one or more of the provisions of this Agreement is unenforceable, the enforceability of the remaining provisions shall be unimpaired

The above terms and provisions are hereby accepted and agreed to by the following Expert and will be effective on the date of execution herein below.

Sincerely,

Bryan Chiles
TASER International, Inc.

ACCEPTED AND AGREED to:

By: ______________________
Bryan Chiles

Date: ______________________

ACCEPTED AND AGREED to:

By: ___________________________
[Name of Client Representative]

____
[Name of Client]

Date: ___________________________

EXHIBIT A
FEE SCHEDULE FOR EXPERT TESTIMONY
Bryan Chiles
TASER INTERNATIONAL, INC.

TASER® | Axon® Device Analysis and Report:
A TASER device analysis and standard report will be billed in accordance with TASER International, Inc.'s current Investigation fee schedule:

	Download Analysis	Full Analysis
M26	$ 250.00	$ 500.00
X26	$ 350.00	$ 700.00
X26 + TASER CAM	$ 550.00	$ 1,000.00
XREP	$ 500.00	$ 1,000.00
X3	$ 900.00	$ 1,800.00
X2	$ 600.00	$ 1,200.00
X2 + TASER CAM HD	$ 800.00	$ 1,400.00
X26P	$ 500.00	$ 1,000.00
X26P + TASER CAM HD	$ 700.00	$ 1,200.00
TASER CAM	$ 350.00	N/A
TASER CAM HD	$ 350.00	N/A
AXON Camera	$ 700.00	N/A
Expedite Fee	$ 500.00	$ 1,000.00

These fees are effective as of the revised date of this document. Please go to http://communities.taser.com/support/InvestigationForm?typ=LE to submit a request for analysis and to see the most current fees.

Additional Compensation:
For work performed in addition to the standard analysis and report (e.g., reviewing additional case documentation, research beyond that needed for a standard analysis, generation of a Rule 26 expert report, testifying at trial or deposition) the hourly billing rate is $200 per hour for time spent actively working on the matter regardless of location. Maximum $1,600 per day bill rate. Travel time is billed at $50 per hour, and idle time is billed at $75.00 per hour, not to exceed $600.00 per day. Travel expenses (including flights, rental cars, parking, lodging and meals) are to be reimbursed. Extended travel expenses due to delays in testimony (change fees, supplies, etc.) are also to be reimbursed.

NON-COLLUSION STATEMENT:

By signing this offer, the vendor/contractor certifies that this offer is made independently and *free* from collusion. Vendor shall disclose below any City of Fort Lauderdale, FL officer or employee, or any relative of any such officer or employee who is an officer or director of, or has a material interest in, the vendor's business, who is in a position to influence this procurement.

Any City of Fort Lauderdale, FL officer or employee who has any input into the writing of specifications or requirements, solicitation of offers, decision to award, evaluation of offers, or any other activity pertinent to this procurement is presumed, for purposes hereof, to be in a position to influence this procurement.

For purposes hereof, a person has a material interest if they directly or indirectly own more than 5 percent of the total assets or capital stock of any business entity, or if they otherwise stand to personally gain if the contract is awarded to this vendor.

In accordance with City of Fort Lauderdale, FL Policy and Standards Manual, 6.10.8.3,

> 3.3. City employees may not contract with the City through any corporation or business entity in which they or their immediate family members hold a controlling financial interest (e.g. ownership of five (5) percent or more).
>
> 3.4. Immediate family members (spouse, parents and children) are also prohibited from contracting with the City subject to the same general rules.

Failure of a vendor to disclose any relationship described herein shall be reason for debarment in accordance with the provisions of the City Procurement Code.

NAME	**RELATIONSHIPS**
______________________________	______________________________
______________________________	______________________________
	______________________________
	______________________________

In the event the vendor does not indicate any names, the City shall interpret this to mean that the vendor has indicated that no such relationships exist.

d. Local Preference Certification

TASER International, Inc. does not qualify for any of the local business preferences described on the following form.

LOCAL BUSINESS PREFERENCE CERTIFICATION STATEMENT

The Business identified below certifies that it qualifies for the local BUSINESS preference classification as indicated herein, and furtl certifies and agrees that it will re-affirm it's local preference classification annually no later than thirty (30) calendar days prior to the anniversary of the date of a contract awarded pursuant to this ITB. Violation of the foregoing provision may result in contract termination.

(1) *Not applicable to TASER.* ____________________
Business Name

is a **Class A** Business as defined in City of Fort Lauderdale Ordinance No. C-12-04, Sec.2-199.2. A copy of the City of Fort Lauderdale current year Business Tax Receipt **and** a complete list of full-time employees and evidence of their addresses shall be provided within 10 calendar days of a formal request by the City.

(2) *Not applicable to TASER.* ____________________
Business Name

is a **Class B** Business as defined in the City of Fort Lauderdale Ordinance No. C-12-04, Sec.2-199.2. A copy of the Business Tax Receipt **or** a complete list of full-time employees and evidence of their addresses shall be provided within 10 calendar days of a formal request by the City.

(3) *Not applicable to TASER.* ____________________
Business Name

is a **Class C** Business as defined in the City of Fort Lauderdale Ordinance No. C-12-04, Sec.2-199.2. A copy of the Broward County Business Tax Receipt shall be provided within 10 calendar days of a formal request by the City.

(4) *Not applicable to TASER.* ____________________
Business Name

requests a **Conditional Class A** classification as defined in the City of Fort Lauderdale Ordinance No. C-12-04, Sec.2-199.2. Written certification of intent shall be provided within 10 calendar days of a formal request by the City.

(5) *Not applicable to TASER.* ____________________
Business Name

requests a **Conditional Class B** classification as defined in the City of Fort Lauderdale Ordinance No. C-12-04, Sec.2-199.2. Written certification of intent shall be provided within 10 calendar days of a formal request by the City.

(6) *Not applicable to TASER.* ____________________
Business Name

is considered a **Class D** Business as defined in the City of Fort Lauderdale Ordinance No. C-12-04, Sec.2-199.2. and does not qualify for Local Preference consideration.

BIDDER'S COMPANY: TASER International, Inc.

AUTHORIZED COMPANY PERSON: Josh Isner, EVP, Global Sales ________________ 10/24/2016
NAME SIGNATURE DATE

CONTRACT PAYMENT METHOD BY P-CARD

THIS FORM MUST BY SUBMITTED WITH YOUR RESPONSE

The City of Fort Lauderdale has implemented a Procurement Card (P-Card) program which changes how payments are remitted to its vendors. The City has transitioned from traditional paper checks to payment by credit card via MasterCard or Visa. This allows you as a vendor of the City of Fort Lauderdale to receive your payment fast and safely. No more waiting for checks to be printed and mailed.

Payments will be made utilizing the City's P-Card (MasterCard or Visa). Accordingly, firms must presently have the ability to accept credit card payment or take whatever steps necessary to implement acceptance of a credit card before the commencement of a contract.

Please indicate which credit card payment you prefer: Either is fine.

✓ Master Card

✓ Visa Card

Company Name: TASER International, Inc.

Josh Isner
Name (printed)

Signature

October 25, 2016
Date:

EVP, Global Sales
Title

CERTIFICATE OF LIABILITY INSURANCE

DATE(MM/DD/YYYY)
10/25/2016

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

Holder Identifier :

PRODUCER
Aon Risk Insurance Services West, Inc.
Phoenix AZ Office
2555 East Camelback Rd.
Suite 700
Phoenix AZ 85016 USA

CONTACT NAME:
PHONE (A/C. No. Ext): (866) 283-7122 FAX (A/C. No.): (800) 363-0105
E-MAIL ADDRESS:

INSURER(S) AFFORDING COVERAGE		NAIC #
INSURER A:	Colony Insurance Company	39993
INSURER B:		
INSURER C:		
INSURER D:		
INSURER E:		
INSURER F:		

INSURED
Taser International, Inc.
17800 N. 85th Street
Scottsdale AZ 85255 USA

COVERAGES CERTIFICATE NUMBER: 570064226064 REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

Limits shown are as requested

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
	□ COMMERCIAL GENERAL LIABILITY □ □ CLAIMS-MADE □ OCCUR □ □ GEN'L AGGREGATE LIMIT APPLIES PER: □ POLICY □ PRO-JECT □ LOC OTHER:						EACH OCCURRENCE DAMAGE TO RENTED PREMISES (Ea occurrence) MED EXP (Any one person) PERSONAL & ADV INJURY GENERAL AGGREGATE PRODUCTS - COMP/OP AGG	
	AUTOMOBILE LIABILITY □ ANY AUTO □ OWNED AUTOS ONLY □ SCHEDULED AUTOS □ HIRED AUTOS ONLY □ NON-OWNED AUTOS ONLY						COMBINED SINGLE LIMIT (Ea accident) BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident)	
	□ UMBRELLA LIAB □ OCCUR □ EXCESS LIAB □ CLAIMS-MADE DED RETENTION						EACH OCCURRENCE AGGREGATE	
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR / PARTNER / EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) Y / N □ If yes, describe under DESCRIPTION OF OPERATIONS below	N / A					PER STATUTE OTH-ER E.L. EACH ACCIDENT E.L. DISEASE-EA EMPLOYEE E.L. DISEASE-POLICY LIMIT	
A	E&O-Technology			EO407121 Cyber & Professional E&O	09/18/2016	09/30/2017	Per Claim Aggregate Deductible	$5,000,000 $5,000,000 $75,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Certificate No : 570064226064

CERTIFICATE HOLDER

City of Fort Lauderdale
Procurement Services Division
100 N. Andrews Avenue, Room 619
Fort Lauderdale FL 33301 USA

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Aon Risk Insurance Services West, Inc.

AGENCY CUSTOMER ID: 570000007117

LOC #:

ACORD®

ADDITIONAL REMARKS SCHEDULE

Page _ of _

AGENCY Aon Risk Insurance Services West, Inc.	NAMED INSURED Taser International, Inc.
POLICY NUMBER See Certificate Number: 570064226064	
CARRIER See Certificate Number: 570064226064 / NAIC CODE	EFFECTIVE DATE:

ADDITIONAL REMARKS

THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,
FORM NUMBER: ACORD 25 FORM TITLE: Certificate of Liability Insurance

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER	
INSURER	
INSURER	
INSURER	

ADDITIONAL POLICIES If a policy below does not include limit information, refer to the corresponding policy on the ACORD certificate form for policy limits.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFFECTIVE DATE (MM/DD/YYYY)	POLICY EXPIRATION DATE (MM/DD/YYYY)	LIMITS	
	OTHER							
	☒ Retro Date 9/18/14							

CERTIFICATE OF LIABILITY INSURANCE

DATE(MM/DD/YYYY)
10/25/2016

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

Holder Identifier :

PRODUCER
Aon Risk Insurance Services West, Inc.
Phoenix AZ Office
2555 East Camelback Rd.
Suite 700
Phoenix AZ 85016 USA

CONTACT NAME:
PHONE (A/C. No. Ext): (866) 283-7122 FAX (A/C. No.): (800) 363-0105
E-MAIL ADDRESS:

INSURER(S) AFFORDING COVERAGE		NAIC #
INSURER A:	Lexington Insurance Company	19437
INSURER B:		
INSURER C:		
INSURER D:		
INSURER E:		
INSURER F:		

INSURED
Taser International, Inc.
17800 N. 85th Street
Scottsdale AZ 85255 USA

COVERAGES CERTIFICATE NUMBER: 570064226058 REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

Limits shown are as requested

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	☒ COMMERCIAL GENERAL LIABILITY			028182385	12/15/2015	12/15/2016	EACH OCCURRENCE	$10,000,000
	☐ ☒ CLAIMS-MADE ☐ OCCUR			GL - Claims Made SIR applies per policy terms & conditions			DAMAGE TO RENTED PREMISES (Ea occurrence)	Excluded
A	☒ Occurrence Policy for Non-ECD			021391643	12/15/2015	12/15/2016	MED EXP (Any one person)	Excluded
	☒ Claims Made Policy for ECD Taser Only			GL - Occurrence			PERSONAL & ADV INJURY	Included
	GEN'L AGGREGATE LIMIT APPLIES PER:			SIR applies per policy terms & conditions			GENERAL AGGREGATE	$10,000,000
	☐ POLICY ☐ PRO-JECT ☐ LOC						PRODUCTS - COMP/OP AGG	$10,000,000
	☒ OTHER:							
	AUTOMOBILE LIABILITY						COMBINED SINGLE LIMIT (Ea accident)	
	☐ ANY AUTO						BODILY INJURY (Per person)	
	☐ OWNED AUTOS ONLY ☐ SCHEDULED AUTOS						BODILY INJURY (Per accident)	
	☐ HIRED AUTOS ONLY ☐ NON-OWNED AUTOS ONLY						PROPERTY DAMAGE (Per accident)	
	☐ UMBRELLA LIAB ☐ OCCUR						EACH OCCURRENCE	
	☐ EXCESS LIAB ☐ CLAIMS-MADE						AGGREGATE	
	☐ DED ☐ RETENTION							
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY						☐ PER STATUTE ☐ OTH-ER	
	ANY PROPRIETOR / PARTNER / EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) Y / N ☐	N / A					E.L. EACH ACCIDENT	
	If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE-EA EMPLOYEE	
							E.L. DISEASE-POLICY LIMIT	

Certificate No : 570064226058

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)
The General Liability Occurrence policy and the Claims Made policy share the limit.

CERTIFICATE HOLDER

City of Fort Lauderdale
Procurement Services Division
100 N. Andrews Avenue, Room 619
Fort Lauderdale FL 33301 USA

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE
Aon Risk Insurance Services West, Inc.

ACORD®

CERTIFICATE OF LIABILITY INSURANCE

DATE(MM/DD/YYYY)
10/25/2016

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

Holder Identifier :

PRODUCER
Aon Risk Insurance Services West, Inc.
Phoenix AZ Office
2555 East Camelback Rd.
Suite 700
Phoenix AZ 85016 USA

CONTACT NAME:
PHONE (A/C. No. Ext): (866) 283-7122
FAX (A/C. No.): (800) 363-0105
E-MAIL ADDRESS:

INSURER(S) AFFORDING COVERAGE		NAIC #
INSURER A:	Twin City Fire Insurance Company	29459
INSURER B:	Hartford Casualty Insurance Co	29424
INSURER C:		
INSURER D:		
INSURER E:		
INSURER F:		

INSURED
Taser International, Inc.
17800 N. 85th Street
Scottsdale AZ 85255 USA

COVERAGES CERTIFICATE NUMBER: 570064226061 REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

Limits shown are as requested

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
	□ COMMERCIAL GENERAL LIABILITY						EACH OCCURRENCE	
	□ □ CLAIMS-MADE □ OCCUR						DAMAGE TO RENTED PREMISES (Ea occurrence)	
	□						MED EXP (Any one person)	
	□						PERSONAL & ADV INJURY	
	GEN'L AGGREGATE LIMIT APPLIES PER:						GENERAL AGGREGATE	
	□ POLICY □ PRO-JECT □ LOC						PRODUCTS - COMP/OP AGG	
	OTHER:							
B	AUTOMOBILE LIABILITY			59 UUN ZM9776	09/30/2016	09/30/2017	COMBINED SINGLE LIMIT (Ea accident)	$1,000,000
	☒ ANY AUTO						BODILY INJURY (Per person)	
	□ OWNED AUTOS ONLY □ SCHEDULED AUTOS						BODILY INJURY (Per accident)	
	☒ HIRED AUTOS ONLY ☒ NON-OWNED AUTOS ONLY						PROPERTY DAMAGE (Per accident)	
	□ □							
	□ UMBRELLA LIAB □ OCCUR						EACH OCCURRENCE	
	□ EXCESS LIAB □ CLAIMS-MADE						AGGREGATE	
	DED RETENTION							
A	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR / PARTNER / EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) Y / N [N] If yes, describe under DESCRIPTION OF OPERATIONS below	N / A		59WEPE1196	09/11/2016	09/11/2017	☒ PER STATUTE □ OTH-ER	
							E.L. EACH ACCIDENT	$1,000,000
							E.L. DISEASE-EA EMPLOYEE	$1,000,000
							E.L. DISEASE-POLICY LIMIT	$1,000,000

Certificate No : 570064226061

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

CERTIFICATE HOLDER

City of Fort Lauderdale
Procurement Services Division
100 N. Andrews Avenue, Room 619
Fort Lauderdale FL 33301 USA

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Aon Risk Insurance Services West, Inc.

State of Florida

IN GOD WE TRUST

Department of State

I certify from the records of this office that TASER INTERNATIONAL, INC., is a corporation organized under the laws of Delaware, authorized to transact business in the State of Florida, qualified on March 25, 2010.

The document number of this corporation is F10000001499.

I further certify that said corporation has paid all fees due this office through December 31, 2010, and its status is active.

I further certify that said corporation has not filed a Certificate of Withdrawal.

Given under my hand and the
Great Seal of the State of Florida
at Tallahassee, the Capital, this the
First day of April, 2010

GREAT SEAL OF THE STATE OF FLORIDA
IN GOD WE TRUST

Kurt S. Browning
Secretary of State

CR2EO22 (01-07)

	ATTACHMENT A - FORT LAUDERDALE POLICE DEP'T (FLPD) BODY WORN CAMERA AND DIGITAL EVIDENCE MANAGEMENT SYSTEM FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS		
Vendor Response Codes			
SF	Standard Functionality ("Out-of-the-Box")		
NR	Provided in Next Release		
MD	Modification Required		
TP	Third Party Software/Hardware Required		
NA	Cannot Meet Requirement		
	(If any vendor response other than **SF,** or if you cannot meet or have an alternate solution please - INCLUDE COMMENTS IN "COMMENTS BOX" BELOW)		
Functional Category: General System			
Reference Number	**Business Requirements**	**Response Code**	**Comments**
GS-1	The Digital Evidence management system should leverage the FLPD's Microsoft Active Directory (AD) for managing system security access and User authentication login/logoff.	**SF**	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, 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.
GS-2	.All recording and storage components should synchronize with an external universal clock, either GPS or another source for absolute time and date to ensure accuracy.	**SF**	Video files generated by the Axon are embedded with metadata, or data about data. Every time an Axon video is created, the date and time of the recording is logged as metadata and embedded in the MP4 file. Any time a camera is docked into the Axon Dock or connected to a computer running Evidence Sync, the time is automatically checked and reset. The dates and timestamps sync with the atomic clocks at the National Institute of Standards and Technology (NIST) and cannot be altered, which protects the chain of custody.
GS-3	Allow officers to review video while in the field and allow video tagging (appending incident details) on the camera device and via a computer device	**SF**	Evidence.com allows for the following indexing fields using Axon View: □ ID –Case ID of incident □ Title –Titles are defaulted to the date and time of the video capture “Flex Video 2012-10-13 1447.” This field can be updated by the user at the time of capture to display a more specific title. □ Category –Allows searching for any category type or to specify any category added by the Agency.
GS-4	All wearable requirements shall be weather resistant in the following conditions and meet IPX2- MIL- STD 810F Method 506.4 procedure 1: • Rain/wind – blown rain Operating temperatures: • -4 to +140 degrees F (-20 to +60 degrees C) Humidity: • 80% non-condensing	**SF**	The **Axon Body 2** is extremely ruggedized, shock-resistant, and water-resistant with a rating of IEC 60529 IP67. These levels of ingress protection (IP) provide users with longer-lasting cameras with fewer failures and overall lower total cost of ownership. The device features complete protection against dust/debris and protection against water immersion at 1 meter for 30 minutes. The Axon Body 2 is also tested to and passes MIL-STD-810G Test Methods (vibration, salt fog, and blowing dust resistance, etc.). -Operating temperature range: −4 °F to 122 °F (−20 °C to 50 °C). -Humidity: 95% non-condensing The **Axon Flex 2** is extremely ruggedized, shock-resistant, and water-resistant with a rating of IEC 60529 IP54. The Axon Flex 2 is also tested to and passes MIL-STD-810G Test Methods (vibration, salt fog, and blowing dust resistance, etc.). -Operating temperature range: −4 °F to 122 °F (−20 °C to 50 °C). -Humidity: 95% non-condensing

Functional Category: General System

Reference Number	Business Requirements	Response Code	Comments
GS-5	Have a drop resistance of at least 6 feet.	**SF**	The devices are impact certified from a height of 6 feet. The most common damage to BWC devices comes as a result of a drop. The Axon Body 2 protects against damage resulting from this common occurrence, providing lower costs associated with damage and downtime. The camera’s magnetic mount is strong enough to hold the camera in place while running or fighting.
GS-6	Have a field view no less than 120 degrees.	**SF**	The **Axon Body 2**’s 143° wide-angle lens was designed to record a wide field of view (FOV) to capture accurate evidence, even when the device is mounted on an officer’s beltline. The Axon Body 2’s horizontal field of view is 107° and the vertical field of view is 78°. The **Axon Flex 2** has a 120° diagonal field of view lens. The horizontal field of view is 102° and the vertical field of view is 55°.
GS-7	Battery should have a minimum recording time of 6 hours.	**SF**	Once powered on, Axon cameras have two operating modes. The default mode, or Buffering mode, provides pre-event buffering to capture activities that occur before you activate the Event (recording) mode. When the device is turned on and in buffering mode, a fully charged battery will last 12+ hours. The Axon Body 2 and Axon Flex 2 video cameras have a minimum video resolution of 480P and a maximum video resolution of 1080P. They utilize an aspect ratio of 16:9 at 1080P and 720P and a 4:3 aspect ratio at 480P. The video resolution, the encoding bitrate, the frame rate and the video encoding format impact the size of the files captured at each setting. The cameras 64GB of non-removable storage. The cameras have four video quality settings, Low SD, High SD, Low HD, High HD spanning 480P, 720P and 1080P video resolutions. □ The Low SD setting captures video at a 480P video resolution at a rate of .81 GB per 60 minutes of video. This allows for over 70 hours of recording □ The High SD setting captures video at a 480P video resolution at a rate of 1.8 GB per 60 minutes of video. This allows for over 35 hours of recording □ The Low HD setting captures video at 720P video resolution at a rate of 2.7 GB per 60 minutes of video. This allows for over 23 hours of recording □ The High HD setting captures video at 1080P video resolution at a rate of 5.4 GB per 60 minutes of video. This allows for 11.3 hours of recording
GS-8	Have a simple camera charging and video offload process..	**SF**	With the Axon Dock, your camera charging station is also your automatic data downloader. At the end of your shift, the Dock syncs video from your Axon camera during routine charging. Videos are uploaded directly to Evidence.com, eliminating manual filing processes and freeing you to focus on more important duties.

Functional Category: General System			
Reference Number	Business Requirements	Response Code	Comments
GS-9	Document the process for charging and downloading video.	SF	The Axon docking station allows for seamless upload and of captured media. At the conclusion of an officer's shift, they will dock their Axon camera into the docking station. Dock and walk. It's that simple. □ A date and time stamp is recorded as metadata and is embedded in the file. Each time the device is docked the time is automatically checked and reset. The time and date cannot be altered, which protects the chain of custody. □ All communication between the Axon docking station will be conducted over 256-bit AES encryption. □ All metadata on the videos captured will be uploaded to Evidence.com. This includes the CAD or RMS incident numbers, categories, and video title. □ A SHA cryptographic hash function is applied to each MP4 video captured on the Axon camera. This functions as a digital fingerprint for each video captured. □ As the MP4 video file is uploaded, it is broken into small blocks of data. At the completion of each block uploading, a SHA hash function is applied to ensure authenticity and that data has uploaded in its entirety. □ In the event of an Internet service interruption, the upload will resume at the last successful block. This includes when an officer must remove their Axon camera from the Dock mid-upload. □ At the completion of the upload, all of the blocks are reconstituted into an exact copy of the original MP4 video captured on the officer's camera. □ The SHA cryptographic hash function is applied to ensure authenticity and that the complete file has uploaded. □ Once files are verified, they are deleted from the Axon camera.
GS-10	Hold a battery life of +12 hours fully charged and stand-by time in buffering. State battery life in detail.	SF	Once powered on, Axon cameras have two operating modes. The default mode, or Buffering mode, provides pre-event buffering to capture activities that occur before you activate the Event (recording) mode.
GS-11	Recharging battery from fully depleted should not exceed 4 hours.	SF	The recharge time for 12+ hours of buffering mode is approximately six (6) hours when a camera with a fully depleted battery is charged in the Axon Dock. Since the cameras have enough battery to last more than a normal shift, the batteries should not be fully depleted regularly and therefore, may take less than 6 hours to charge.
GS-12	Should have a download/charging station for multiple cameras that allows both functions to be completed simultaneously. The charging options shall include: • USB • Wall charger • Vehicle charger Indicate how many cameras per station: Provide technical and physical specifications for stations.	SF	The recommended method of charging is via the Axon Dock. You can also use a wall charger or computer to charge the battery via a USB to 2.5mm connector cable. TASER is able to also provide suitable in-vehicle USB chargers for use with cigarette lighters. Using a non-TASER approved wall charger may degrade device performance and will void the warranty. A fully charged camera battery should provide enough power for approximately 12 hours of normal operation. Recharging a battery after a 12-hour use can take up to 6 hours if you are recharging your Axon camera from a wall outlet or Axon Dock. Recharging could take considerably longer if you are recharging from a computer. If the battery depletes significantly during use, you will hear 4 quick tones repeating every 5 minutes. This message indicates that less than approximately 20 percent of the battery capacity remains. Always recharge a depleted battery as soon as reasonably possible. Each Axon Dock can charge up to six (6) Axon units simultaneously. Additional docks can be purchased to have a 1:1 dock to camera ratio. Please see the attached docking station spec sheets, included as appendices.
GS-13	All wearable components requiring battery should be rechargeable.	SF	Axon batteries are rechargeable.

Functional Category: General System

Reference Number	Business Requirements	Response Code	Comments
GS-14	Wearable devices should provide a configurable audio-visual or haptic cue when activated. Status for the following: • Recording • Deactivation of recording	SF	The Axon Body 2 camera and Axon Flex 2 controller provide a clear visual indication the device is recording in the form of an LED light, located on the top of the unit. While recording, the LED will blink red to clearly indicate that the device is recording; the device's LED blinks green, the camera is in buffering mode.
GS-15	Any illuminated/audible controls or indicators should have a user option which allows them to be extinguished during a tactical/darkness/other situation.	SF	For some situations, an officer may wish to turn off the lights on the Axon 2. You can turn off the lights through the Evidence Sync software application or by using the Battery button. To turn the lights off using the Battery button: □ Press and hold the Battery button for 10 seconds. To turn the lights back on: □ Press and hold the Battery button for 10 seconds. To use Evidence Sync: 1. Connect the camera to the Evidence Sync application. 2. Select the device settings. 3. Select the option to turn off the device LEDs. o The Operation LED flashes red, yellow, and then green before shutting down the lights. o Pressing the Battery button will momentarily light both the Operation LED and the Battery LED, displaying the current operating mode and battery level. To turn the lights back on: 1. Connect the camera to the Evidence Sync application. 2. Select the device settings. 3. Select the option to turn on the device LEDs.
GS-16	Have the ability to control volume of audible status cue to mute, vibrate, etc.	SF	By pressing the volume/pairing button on the camera, an officer can adjust the volume of the camera's audible prompts. The volume has four settings: □ Low □ Medium □ High □ Off At each level, the camera beeps, provide you with a sample of the volume. Pressing the volume escalates the system from lowest to highest, and then off. Other than the audio prompt beeps heard on the audio recordings, the volume/pairing button has no effect on the audio recording captured by the camera.
GS-17	Have the capability for capturing GPS coordinates. Explain methodology in comments.	SF	While Axon cameras do not have built-in GPS capabilities, GPS tagging is available via TASER's free mobile application, Axon View. When installed on an officer's smart device and paired to his or her camera via a Bluetooth connection, Axon View allows the camera to source GPS location information from the mobile device and automatically tag the video file with a GPS location. When a new coordinate is received by the smart device, the coordinates are sent to the camera system. The metadata is pulled directly from the smart device's GPS coordinates and the location is then geo-tagged in Evidence.com. Metadata and watermarks are visible when viewing a video in Evidence.com.

Functional Category: General System

Reference Number	Business Requirements	Response Code	Comments
GS-18	Vendor shall provide 24/7 call center and technical support including initiation of camera replacement. Onsite support is available as required by priority/severity	SF	TASER has a full customer support division; live phone support is available Monday-Thursday, 6:00AM – 12:00AM (Arizona Time), Friday, 6:00AM – 5:00PM and Sunday, 4:00PM – 12:00AM. Critical Incident/Emergency assistance is available 24/7. For technical or Customer Service assistance, you may contact a customer service representative via phone or via email. You may also submit a case to our Customer Service department at any time through our Website TASER.com. From the “Help” section in Evidence.com, you can access our Help Center which includes general information and FAQs. Product User Guides and Evidence.com update release notes are also available for download. You may also contact support from the Evidence.com Help Center. An email will be generated and sent to our Customer Service team and you will be contacted by a representative either by phone or email, based on your preferred contact method. If at any point an issue needs to be escalated, we have a support team in place. All submitted cases through our site will be addressed within 2 business days. The following describes our levels of support available in priority or tiers: **Tier 1 Technical Support - General how-to questions:** □ Frequently asked questions (FAQs) □ Product navigation □ Feature clarification □ Standard queries □ Assistance with known solutions **Tier 2 Technical Support:** □ Advanced Product trouble shooting □ Advanced Evidence.com Configuration □ Any Escalated issues from Tier 1 support **Tier 3 Technical Support:** □ Critical problem or recurring problems rendering the product inoperable or requiring workarounds, bug fixes, testing and/or simulation
GS-19	Have the capability if docked to self-assign the device to the current logged in user based on Active Directory log in.	SF	Axon cameras can be shared among personnel and assigned to different shifts, but TASER does not recommend the “pool of cameras” workflow. We recommend fully deploying cameras to each officer instead of checking cameras in and out using an AD log in. An administrator can assign devices to individuals using the unique serial number of each camera. Officer information is not directly embedded into the video files encoded on the Axon camera; associations are made between an officer and the camera assigned to them. When files from the camera are ingested into Evidence.com, they are automatically populated with metadata indicating to whom the camera belongs. The account administrator is the starting point for defining security settings, creating custom roles and setting permissions, adding users (User, Administrator, Armorer or any other custom roles), reassigning devices, creating categories and setting retention policies, and several of the other administrative features of the Evidence.com services.
GS-20	Software should prompt the current user, if docked, to change device assignment if different than the user currently assigned to the device.	SF	The software will prompt the current user to change device assignment if different than the user currently assigned to the device.

Functional Category: General System			
	Business Requirements		Comments
Reference Number		Response Code	
GS-21	Be compatible with industry standard browsers: Please list browser compatibility for video review and system administrator, and any other functions.	SF	TASER supports the use of Evidence.com with the following web browsers: □ Internet Explorer version 10 and above Note: If you use Internet Explorer, ensure that Compatibility View is disabled. Evidence.com does not support the use of the Compatibility View feature. To verify your Internet Explorer settings, go to Tools > Compatibility View settings and ensure that Evidence.com is not included in the list of websites added to Compatibility View and that the “Display all websites in Compatibility View” check box is cleared. □ Chrome version 40 and above □ Firefox version 30 and above □ Safari version 8 and above Additionally, TASER supports the media player and related tools, introduced in Evidence.com release 1.27, with the following web browsers: □ Internet Explorer version 10 and above □ Chrome version 43 and above □ Firefox version 38 and above □ Safari version 8 and above If you use an unsupported browser to access media-evidence files, Evidence.com provides the traditional media player. It is strongly recommended that you always use the latest release of Adobe Flash.
GS-22	Should have mode indicators that include: • Storage space • Battery strength • Power on	SF	**Storage Space** - The device’s internal firmware is constantly checking the remaining storage capacity. Should recording capacity drop below 6 GB of available storage - the device will emit three quick successive beeps, these beeps will repeat every 15 minutes. In addition, the "Function LED" will blink yellow. When recording capacity has been reached, the device will beep three times and every time the user attempts to start a new event, will beep three times and not enter recording mode. The device will never overwrite over any previously recorded footage. It is not possible to delete, modify or overwrite any video content on the device; it can only deleted once it has been successfully transferred to Evidence.com. This ensures that no data is accidentally deleted or modified on the device. The device features 64GB of storage capacity. The device features sufficient storage for 11-70 hours of recording. It is only under extreme circumstances that the device would have low remaining capacity. **Battery Strength** - An officer can determine the remaining battery life of the camera by pressing the Battery Status button. The button is located beneath the camera’s Event button on the front of the device. The Battery LED ring displays the battery’s remaining capacity when the device is in used or when charging. □ Battery capacity is 41 –100 percent - Solid green □ Battery capacity is 20 –40 percent - Solid yellow □ Battery capacity is less than 20 percent - Solid red during operation; flashing red and yellow during charging □ Battery is critically low - Blinking red and yellow If the battery depletes significantly during use, you will hear 4 quick tones repeating every 5 minutes. This message indicates that less than approximately 20 percent of the battery capacity remains. Always recharge a depleted battery as soon as reasonably possible. **Power on**- When the camera’s power is turned on, the red portion or the on/off indicator is exposed. When the camera power is turned off, the red portion is covered from view.

Functional Category: General System

Reference Number	Business Requirements	Response Code	Comments
GS-23	Have the ability to burn CD/DVD of video footage by request of authorized users and prove authenticity if challenged in court.	**SF**	A User can access a file on Evidence.com, download the file, and then copy it to a CD/DVD or flash/thumb drive. DVDs and CDs can be created using any DVD or CD writing software. Axon cameras record using MP4 format, which is playable without the need for proprietary software.
GS-24	Have the ability to play back recording in most standard DVD players and/or PC's after user authentication is provided.	**SF**	A User can access a file on Evidence.com, download the file, and then copy it to a CD/DVD or flash/thumb drive. DVDs and CDs can be created using any DVD or CD writing software. Axon cameras record using MP4 format, which is playable without the need for proprietary software.
GS-25	Playback should be in a standard non-proprietary format.	**SF**	Video and audio are recorded and exported to the application in a standard, open, and non-proprietary format, including both codec and container. Audio and video are recorded as the same MP4 encoded file ensuring perfect synchronization. The video format is MPEG4 using the H.264 compression standard. Sound is recorded via the Advanced Audio Coding (AAC) coding standard for lossy digital audio compression. The MP4 files can be played using all freely available standard software (i.e. Windows Media player, Real player, QuickTime, VLC, etc.).
GS-26	System should ensure the video has been successfully uploaded prior to deletion from the device. Explain checksum, hash calculation or any other method of verification in comments.	**SF**	Videos are not deleted from the Axon camera until the files are successfully uploaded to Evidence.com. Once the camera is docked in the Axon Dock, an encrypted 256-bit AES SSL session is established with the local storage device and videos are then sorted and uploaded automatically. As a video is being downloaded, it is broken into small blocks of approximately 2-3 megabytes in size. Prior to upload the block is hashed using the SHA algorithm to generate a unique fingerprint or checksum. The block is then downloaded and upon receipt the block is hashed again using the SHA algorithm, if an identical checksum is generated then the file's fingerprints match and the block is unaltered from its original state on the Axon. The dock uploads one file from one camera at a time, then moves on to the next file on that camera. Once the first camera's files have all been transported to Evidence.com, the dock begins uploading the next camera's files. The block upload process is repeated until the entire MP4 is transferred. Using the same method that was used to validate the blocks, a contiguous checksum of the entire file will be evaluated to ensure that the MP4 file has been uploaded successfully and identical to when it was recorded. Once Evidence.com confirms receipt, the video is deleted from the camera and the upload process moves to the next file.

Functional Category: General System

Reference Number	Business Requirements	Response Code	Comments
GS-27	Technology warranty options to replace existing hardware and software for each major feature release or at set intervals over product lifetime according to warranty chosen.	SF	Standard Manufacturer Warranty TASER warrants that its law enforcement hardware products are free from defects in workmanship and materials for a period of one (1) year from the date of receipt. TASER-Manufactured Accessories are covered under a limited 90-day warranty from the date of receipt. Non-TASER manufactured accessories are covered under the manufacturer's warranty. Extended Warranty There are extended warranties available, which will cover the hardware for 3 years total (1 year manufacturer's warranty plus 2 years extended). The TASER Assurance Plan (TAP) The TASER Assurance Plan (TAP) includes the extended warranty coverage described above, as well as spare products and upgraded models at the end of the TAP Term. The TASER Assurance Plan (TAP) is bundled into the purchase price of the Ultimate and Unlimited Plan Evidence.com licenses. The TAP includes Axon camera upgrades every 2.5 years, TASER's extended warranty and spare cameras. The TASER Assurance Plan (TAP) includes the extended warranty coverage described in the current hardware warranty, as well as spare products and upgraded models at the end of the TAP Term. TAP does not apply to software or services offered for, by, on, or through the TASER.com or Evidence.com websites. You may not have both an optional extended warranty and TAP on Axon products. Software Upgrades and Updates The latest product features and enhancements are included as part of your investment in Evidence.com. Software is updated regularly throughout the year, and these updates are included in the price of your software licenses.
GS-28	Have the ability to upload to backend archivers via WiFi.	NR	The Axon is equipped with Wi-Fi 802.11n at 5 GHz and 2.4 GHz. In 2017, this connectivity will be enhanced to enable the camera to automatically offload videos when pre-configured Wi-Fi network are available.
GS-29	Have automated triggers to activate recordings using WiFi and/or Bluetooth. Examples: - Emergency Light - Vehicle Impact - Firearm withdrawl from holster - Vehicle Speed Threshold	NR	The Axon Signal operates over Bluetooth Low Energy and triggers recording of Axon cameras via various triggers (including Axon Fleet, Axon Body 2 and Signal-enabled Axon Flex cameras). The effective range of Axon Signal is up to 30ft (~10 meters). The Axon Signal products that we offer today are the Axon Signal Unit and Signal Performance Power Magazine. Here's how they work: □ Axon Signal Unit (ASU): Activate your camera with vehicle triggers, like light bar, door, and weapon rack. Ideal for cars, SUVs, and motorcycles. □ Signal Performance Power Magazine (SPPM): Capture critical footage when you use your X2 and X26P Smart Weapons. SPPM activates your camera when your weapon is armed, trigger is pulled and arc is engaged.
GS-30	Include iOS and Android mobile apps for 'Live' view and/or post video viewing	SF	Axon View is a free mobile application that wirelessly connects with your Axon camera to provide instant playback of unfolding events from the field, in the field. You can use the app's live display to ensure your camera is well-placed, and the playback function helps eliminate the "he said, she said" on the spot. GPS markers are automatically added to videos captured with the Axon when paired to a smart device with GPS capabilities. Evidence.com allows for the following indexing fields using Axon View: □ ID – Case ID of incident □ Title – Titles are defaulted to the date and time of the video capture "Flex Video 2012-10-13 1447." This field can be updated by the user at the time of capture to display a more specific title □ Category – Allows searching for any category type or to specify any category added by the Agency.

Functional Category: General System			
	Business Requirements		Comments
Reference Number		Response Code	
GS-31	Storage shall be hosted by the vendor. Please describe exactly how all costs are calculated for any use of the system including: - Upload - Storage - Download - Access - Any other storage cost	**SF**	Agencies are charged for hardware including cameras, docking stations and camera mounts. Software is included in the purchase price of camera licenses. License tiers available are outlined in the Evidence.com product specifications, included as an appendix.
GS-32	Should be CJIS compliant for the storage solution	**SF**	TASER acknowledges and abides by all aspects of the CJIS Security Addendum. CJIS Security Addendum Certification pages are maintained for each authorized TASER employee and are available to customers. Authorized TASER employees are available for state of residence and national fingerprint-based record checks at either the state or local level and are available to complete state specific security awareness training. Additionally, TASER adheres to the audit requirements of the FBI CJIS Security Policy.
GS-33	Shall maintain all data, video, multimedia files in the United States	**SF**	For customers residing in the, United States TASER will ensure that all content stored in Evidence.com remains within the United States including any backup data, replication sites, and disaster recovery sites. Evidence.com customer data is stored within Microsoft Azure Government data centers located in Boydton, VA and Des Moines, IA. Each data center offers world-class security and system protection. Data centers employ backup power, climate control, alarms, and seismic bracing. In the event of a disaster, the system will failover automatically to the secondary site and provide uninterrupted service to customers, providing uninterrupted access during disaster events.

	ATTACHMENT A - FORT LAUDERDALE POLICE DEP'T (FLPD) BODY WORN CAMERA AND DIGITAL EVIDENCE MANAGEMENT SYSTEM FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS				
Vendor Response Codes					
SF	Standard Functionality ("Out-of-the-Box")				
NR	Provided in Next Release				
MD	Modification Required				
TP	Third Party Software/Hardware Required				
NA	Cannot Meet Requirement				
	(If any vendor response other than SF, or if you cannot meet or have an alternate solution please - INCLUDE COMMENTS IN				
	"COMMENTS BOX" BELOW)				
Functional Category: CAMERA					
Reference Number	**Business Requirements**	**Response Code**			**Comments**

Functional Category: CAMERA			
Reference Number	Business Requirements	Response Code	Comments
CA-1	Cameras should have the ability to be mountable on several locations including, but not limited to: • Shoulder • Helmet • Collar • Center of uniform just below neck level • Epaulet Explain in the comments any exceptions	**SF**	The purchase price of each Axon Body 2 camera includes two of the following mounts of FLPD's choice. Additional mounts are available a la carte as listed below. 74018 Z-Bracket, Men's, Axon Body 2 - $29.95 each 74019 Z-Bracket, Women's Axon Body 2 - $29.95 each 74020 Magnet, Flexible, Axon Body 2 - $29.95 each 74021 Magnet, Outerwear, Axon Body 2 - $29.95 each 74022 Small Pocket, 4″ (10.1 cm), Axon Body 2 - $29.95 each 74023 Large Pocket, 6″ (15.2 cm), Axon Body 2 - $29.95 each 11507 Single Molle Mount, Axon Body 2 - $29.95 each 11508 Double Molle Mount, Axon Body 2 - $39.95 each 11509 Clip Mount, Axon Body 2 -$29.95 each The purchase price of each Axon Flex 2 camera includes two of the following mounts of FLPD's choice (excluding the Oakley Flak Jacket Sunglass Mount). Additional mounts are available a la carte as listed below. □ 11544 Oakley Flak Jacket Kit, Flex 2 - $149.00 each □ 11554 Clip, Oakley, Flex 2 - $9.00 each □ 11545 Collar Mount, Flex 2 - $29.00 each □ 11546 Epaulette Mount, Flex 2 - $29.00 each □ 11547 Ball cap Mount, Flex 2 - $19.00 each □ 11555 Ballistic Vest Mount, Flex 2 - $19.00 each □ 11548 Universal Helmet Mount, Flex 2 - $19.00 each □ 11549 Tactical SWAT Kit, w/ ARC Rail, Flex 2 - $49.00 each □ 11561C-Clip Adaptor, Flex 2 - $9.00 each □ 11509 Clip Mount, Rapidlock - $19.95 each
CA-2	Does the camera have a retina low light capability of ≤1 lux.	**SF**	The Axon has Retina Low-Light capability less than 0.1 lux.

Functional Category: CAMERA			
Reference Number	Business Requirements	Response Code	Comments
CA-3	Have capability of capturing still shot images from software/video and export in the following formats: • JPEG • TIFF • BMP • PNG Explain exceptions in the comments	**SF**	**On Camera -** A still image can be captured by using the Function Button on the Axon Body 2 camera and the Axon Flex 2 controller. Pressing the Function Button places a marker at that specific point in the video. At each marker, a thumbnail image is created in the video in Evidence.com. The image will download as a .jpg file. **Axon Capture -** Because still photos are often taken in lower stress situations, officers can also utilize TASER's free mobile application, Axon Capture, to take still photos in the field. Additionally, the application allows a user to capture videos and audio recordings in the field, annotate them, and upload them to Evidence.com. Still images can also be taken from Axon videos within Evidence.com. **Evidence.com -** Users can create a snapshot or still photo from a video in Evidence.com by creating a marker. Simply pause the video on the frame you wish to produce a snapshot from and click the "marker" icon below the playback window. Once a marker is created, you can download the snapshot and edit/add metadata like a title and description. The default video resolution is 640x480 and any still image taken from a video within Evidence.com will be saved as this resolution. When a user downloads the marker from Evidence.com, the image will be in a .jpg format. Evidence.com is source agnostic and can support any digital format. For playback and editing tools, the supported formats are JPEG, JPG, GIF, PNG, BMP.
CA-4	Device storage capacity shall contain at least 8GB of Solid State Memory.	**SF**	The cameras have 64 GB of solid state memory.
CA-5	Ability to integrate secondary prisoner transport camera.	**NA**	Axon cameras do not have the ability to integrate secondary prisoner transport cameras.

Functional Category: CAMERA			
Reference Number	Business Requirements	Response Code	Comments
CA-6	The total number of wire or cable connections for the worn devices **shall not** exceed one cable on the body.	**SF**	The Axon Body 2 is a self-contained audio-visual unit with no external wires. The Axon Flex 2 camera is connected to the Flex controller, which also houses the battery, with one 2.5 mm cable.
CA-7	Shall have camera data storage that is secure and non-removable by the enduser. Explain methodology.	**SF**	All Axon video data is securely stored on a solid-state, non-removable, embedded Multimedia Card (eMMC) inside the Axon device. Rather than using an SD card, the media is populated directly on the circuit board, providing several levels of physical and virtual security. Level 1: Non-standard connection & sealed compartment The camera uses a non-standard connection, thus preventing access to the storage without destruction of the device. Level 2: eMMC Storage - eMMC storage is populated on the circuit board rather than using an SD card. Accessing and reading eMMC is difficult and would require destruction and/or modification of the circuit board. Level 3: No Partition Table - The storage media does not have a partition table and will show as an unreadable drive/card (under any operating system). Level 4: Encryption The data stored on the camera is secure and can be encrypted by means of 256-bit AES encryption. The camera does not allow any footage to be deleted, overwritten, or otherwise modified.

Functional Category: CAMERA			
Reference Number	Business Requirements	Response Code	Comments
CA-8	Camera storage **shall prevent end users from** copying, deleting, tampering, modifying video including using any third party tools. Requires DEMS or proprietary access to memory card – no third party tool access allowed.	**SF**	An officer cannot delete, alter or edit, the videos; he or she can only change the metadata. The integrity of the original data can never be altered. Video content encoded onto the camera is not encrypted since the storage card is non-removable. Encryption only takes place when video content is uploaded to Evidence.com. Evidence.com uses strong encryption to protect Evidence data in transit and at rest. ☐ FIPS 140-¬2 approved encryption ciphers (or stronger) ☐ Robust SSL/TLS implementation for data in transit. o RSA 2048 bit key o TLS 1.2 with 256 bit connection o Perfect Forward Secrecy ☐ 256 bit AES encryption for evidence data in storage Connecting an Axon camera to a PC will not reveal any of the captured content and cameras will not natively mount into a Microsoft Windows operating system like a mass storage device (i.e. flash drive or external hard drive). Axon video footage can only be accessed using Evidence Sync; the video will transfer in an MP4 format and can then be uploaded to an agency's Evidence.com account.

Functional Category: CAMERA			
Reference Number	Business Requirements	Response Code	Comments
CA-9	The device should not overwrite existing data before it has been transferred. Can the system export a hash value of files being transferred? Explain the overwrite protection method.	**SF**	The device will never overwrite over any previously recorded footage. It is not possible to delete, modify or overwrite any video content on the device; it can only deleted once it has been successfully transferred to Evidence.com. This ensures that no data is accidentally deleted or modified on the device. Videos are not deleted from the Axon camera until the files are successfully uploaded to Evidence.com. Once the camera is docked in the Axon Dock, an encrypted 256-bit AES SSL session is established with the local storage device and videos are then sorted and uploaded automatically. When using an Axon Dock to upload videos Axon cameras to Evidence.com, the data is cut into pieces, hashed, and then confirmed whole before the data is deleted from the camera. Prior to upload the block is hashed using the SHA algorithm to generate a unique fingerprint or checksum. The block is then downloaded and upon receipt the block is hashed again using the SHA algorithm, if an identical checksum is generated then the file's fingerprints match and the block is unaltered from its original state on the Axon. The dock uploads one file from one camera at a time, then moves on to the next file on that camera. Once the first camera's files have all been transported to Evidence.com, the dock begins uploading the next camera's files. The block upload process is repeated until the entire MP4 is transferred. Using the same method that was used to validate the blocks, a contiguous checksum of the entire file will be evaluated to ensure that the MP4 file has been uploaded successfully and identical to when it was recorded. Once Evidence.com confirms receipt, the video is deleted from the camera and the upload process moves to the next file.

Functional Category: CAMERA			
Reference Number	Business Requirements	Response Code	Comments
CA-10	Should employ standard encryption such as AES	**SF**	Evidence.com uses strong encryption to protect Evidence data in transit and at rest. □ FIPS 140-¬2 approved encryption ciphers (or stronger) □ Robust SSL/TLS implementation for data in transit. o RSA 2048 bit key o TLS 1.2 with 256 bit connection o Perfect Forward Secrecy □ 256 bit AES encryption for evidence data in storage
CA-11	Should have image stabilization capability	**NA**	Axon cameras are equipped with automatic focus, exposure, and white balance. The devices also utilize automatic image quality control, which adjusts the image parameters dynamically. Axon cameras do not provide Electronic Image Stabilization (EIS), Optical Image Stabilization (OIS) or Mechanical Image Stabilization (MIS). The use of image stabilization has adverse effects on the data within the video file, thereby negatively impacting the ability to forensically analyze a video in an investigation. Axon body-worn cameras are also designed to attach to the officer's uniform in such a way as to minimize the impact and effect of jostling and bouncing, reducing the need to image stabilization.
CA-12	Streaming Live View capability (Explain)	**SF**	Officers can pair their Axon camera to a smart device through Bluetooth connectivity to view and annotate video using the Axon View mobile application. Axon View is a free software application available through the Google Play Store for Android devices, and through iTunes for Apple iOS smart devices (such as iPhone and iPad devices, and multimedia players).

Functional Category: CAMERA			
Reference Number	Business Requirements	Response Code	Comments
CA-13	Shall support MP3 audio format	**SF**	The Axon's minimum audio capture rate is 16-bits to mimic the range of sound an officer in the field would be able to hear. 24 bit audio capture requires higher power and more storage space. The camera does not provide a secondary MP3 or WAV file, as the audio is captured as part of the MP4 video container. If the FLPD wishes to generate a separate audio file, they may use a third party tool to extract the audio from the MP4 video to create an MP3 or WAV file. Using the redaction feature in Evidence.com, you can redact the entire visual portion of the video leaving on the audio, by masking the entire frame (rather than just a face or object within the frame). Evidence.com supports MP3, WAV and AAC audio formats.

Functional Category: CAMERA

Reference Number	Business Requirements	Response Code	Comments
CA-14	Administrators should be able to configure video settings or have selectable bit rate (multiple settings to allow optimization of file size and upload speed).	**SF**	The Axon video camera has a minimum video resolution of 480P and a maximum video resolution of 1080P. It utilizes an aspect ratio of 16:9 at 1080P and 720P and a 4:3 aspect ratio at 480P. The video resolution, the encoding bitrate, the frame rate and the video encoding format impact the size of the files captured at each setting. The camera has 64GB of non-removable storage. The camera has four video quality settings, Low SD, High SD, Low HD, High HD spanning 480P, 720P and 1080P video resolutions. □ The Low SD setting captures video at a 480P video resolution at a rate of .8 GB per 60 minutes of video. This allows for over 70 hours of recording □ The High SD setting captures video at a 480P video resolution at a rate of 1.8 GB per 60 minutes of video. This allows for over 35 hours of recording □ The Low HD setting captures video at 720P video resolution at a rate of 2.7 GB per 60 minutes of video. This allows for over 23 hours of recording □ The High HD setting captures video at 1080P video resolution at a rate of 5.4 GB per 60 minutes of video. This allows for 11.3 hours of recording
CA-15	Shall support a video frame rate of 30 FPS.	**SF**	The Axon records at a rate of 30 frames per second (FPS).
CA-16	Shall have a minimum resolution size of 640 x 480 and a max of 4K.	**SF**	The camera records at 640 x 480 VGA video resolution. The max resolution is 1080p. Axon cameras do not have 4K resolution and we are unaware of any competitors that utilize 4K.

Functional Category: CAMERA			
Reference Number	Business Requirements	Response Code	Comments
CA-17	Describe what the max record time is for each resolution: • 640 X 480 • 1080p • 720p • 4K	**SF**	The camera records at 640 x 480 VGA video resolution. The max resolution is 1080p. Axon cameras do not have 4K resolution and we are unaware of any competitors that utilize 4K. The camera has a minimum video resolution of 480P and a maximum video resolution of 1080P. It utilizes an aspect ratio of 16:9 at 1080P and 720P and a 4:3 aspect ratio at 480P. The video resolution, the encoding bitrate, the frame rate and the video encoding format impact the size of the files captured at each setting. The Axon Body 2 has 64GB of non-removable storage. The camera has four video quality settings, Low SD, High SD, Low HD, High HD spanning 480P, 720P and 1080P video resolutions. □ The Low SD setting captures video at a 480P video resolution at a rate of .8 GB per 60 minutes of video. This allows for over 70 hours of recording □ The High SD setting captures video at a 480P video resolution at a rate of 1.8 GB per 60 minutes of video. This allows for over 35 hours of recording □ The Low HD setting captures video at 720P video resolution at a rate of 2.7 GB per 60 minutes of video. This allows for over 23 hours of recording □ The High HD setting captures video at 1080P video resolution at a rate of 5.4 GB per 60 minutes of video. This allows for 11.3 hours of recording

Functional Category: CAMERA

Reference Number	Business Requirements	Response Code	Comments
CA-18	System should allow administrators to configure pre-event video buffer to range from buffer of zero (off) up to at least 30 seconds prior to recording start.	**SF**	The Axon's pre-event buffer is configurable from 0-120 seconds (in 30 second increments) and features configurable on/off audio capture to record the evidence your agency's needs. There are several cameras on the market that provide a pre-event buffer. The TASER solution is unique in that it also provides the battery life necessary to utilize the buffer for the duration of the officer's shift. Pre-event buffer for the duration of the officer's shift ensures that digital evidence can be captured at any time. Permission to adjust pre-event buffer settings is dependent on the FLPD. Appropriate permissions are important for the best user experience.
CA-19	System should allow administrators to configure pre-event audio to be off	**SF**	At the administrative level, audio recording can be disabled on the Axon by configuring the video settings. Microphone controls are intended for agencies in locations with restrictions on audio recordings. The Microphone setting determines the initial setting when an Axon device is checked out. Administrators can set it to 'Microphone initially on' or 'Microphone initially off'. The device Audit Trail will state whether the microphone was on or off during each recording. **Audio On/Off During Event Recording** By pressing and holding the function button on the device for three seconds, an officer can mute the audio portion of the video capture. By pressing and holding the function button on the device for another three seconds, the audio portion of the recording will be re-enabled.

Functional Category: CAMERA

Reference Number	Business Requirements	Response Code	Comments
CA-20	Have a manual activation method preventing accidental activation or deactivation of recordings. The sequence for activation and deactivation shall be different. Device should provide user feedback indicating activation status. Describe both methods.	**SF**	By design, Axon body-worn cameras require deliberate activation through the use of the Event button. To prevent inadvertent activations, the Event button must be depressed twice and deactivation requires a five second depression. Activation of event recording is simple and accessible, so officers can operate the device in a high-stress situation. Recordings are initiated with a single “Event Button” located on the front of the device, so an officer can easily reach it with one hand. The camera has two operating modes: 1. BUFFERING (turning on the camera and starting pre-event buffering) 2. EVENT (event recording) To initiate Buffering Mode (turn the camera on) Move the ON/OFF switch on the camera to the ON position. The raised on/off switch is strong enough to prevent accidentally powering the device down, yet can still be switched on if an officer is wearing gloves. To initiate Event Recording Mode, simply tap the large concave button on the front of the camera two times. While the device is easily activated when worn in a shirt pocket or housed in a case, it is still protected against unintentional event triggering. To end the recording, simply hold down the button for three seconds.

Functional Category: CAMERA

Reference Number	Business Requirements	Response Code	Comments
CA-21	Have the capability to have in-field review of audio and video and bookmark assignment.	**SF**	Pressing the Function Button on the device during recording places a marker or bookmark at a specific point in the video. You can use TASER's free mobile application Axon View to tag the videos you record with metadata, such as ID, title, and retention category. Axon View transfers the tag information to the Axon camera. Tag information that you apply does not alter the original video evidence file. When you place the Axon camera in an Axon Dock or connect the Axon camera to a computer that is running the Evidence Sync application, the videos on the camera automatically upload to your Evidence.com agency. The tag information that you apply to each video also uploads and can be viewed by anyone with permission to view the evidence. GPS metadata is captured when an officer pairs his or her Axon camera to an Android or iOS smart device running TASER's free mobile application, Axon View. Using a Bluetooth connection, the Axon will source GPS location information from the mobile device. When a new coordinate is received from a paired device, the coordinates are sent to the camera system.

Functional Category: CAMERA			
Reference Number	Business Requirements	Response Code	Comments
CA-22	Have the capability to automatically assign metadata from the dispatched call for service (via in-car computer, Motorola radio, etc).	**SF**	Axon body-worn cameras can interface with your Agency CAD/RMS system. Integrating a CAD/RMS system with Evidence.com provides the FLPD the ability to use either an event number from CAD system or a case number from an RMS system, or a mixture of both with a written statement for handling the data. The solution is provider agnostic, and the printout required for tagging and categorization is queried directly from the database, effectively bypassing the CAD/RMS front-end interface. TASER integrations is an option for any system that has an accessible back-end database (SQL DB, etc.). Often these reports are already pulled for crime statistics reporting. TASER's solution enables automatic tagging of Axon videos with the correct Incident ID, Category, and Location. Automatic retention is accomplished through categorization mapping. TASER's solution uses a proprietary algorithm written to compare CAD/RMS call start and end times with Axon video recording start and end times by officer identifier. TASER supplies a small integrator application that automatically encrypts the automated database printout, sends to Evidence.com via SSL port 443 and then deletes the file from the local server. Automatic tagging occurs once daily with the ability to tag videos from the previous 72-hours.

Functional Category: CAMERA			
Reference Number	Business Requirements	Response Code	Comments
CA-23	Have the capability to allow the enduser to manually tag incident data to the video. Including: - Incident Case Number - Incident Type (Burglary, Disturbance, Field Interview, etc) - Video Location - Arrest: Y/N - Force Used: Y/N - Agency Defined Fields	**SF**	By enabling officers to annotate Axon video with meta-data, Evidence.com turns what was once an overwhelming amount of files and information into a database of highly searchable evidence. Text Search - For evidence searches, the ID, Title, and Tag filters provide advanced text matching features. □ The text you enter can match any part of the data you are filtering. For example, if you enter 21 in the ID box, any evidence whose ID includes “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. For example, if you enter 21 78 in the ID box, search results include evidence with the ID 213789 as well as 421278. □ 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 213789. Evidence Metadata Fields □ ID — Limits search results to evidence whose ID includes the characters you enter in the ID box. □ Title — Limits search results to evidence whose title includes the characters you enter in the Title box. □ Category — Limits search results to evidence that is assigned to the category that you select. By default, search results include evidence assigned to any category, including uncategorized evidence.

Functional Category: CAMERA			
Reference Number	Business Requirements	Response Code	Comments
			□ Date — Limits search results by either the recorded, uploaded, or deletion date of evidence, as selected. You must also specify a date range by using the From and To boxes, else the search is not limited by date range. Search results are inclusive of the dates specified. o From — The start of the date range. If the From box is empty, the date range begins with the earliest possible date. o To — The end of the date range. If the To box is empty, the date range ends with today. □ File Type — Limits search results to the file type selected. By default, search results include all file types. □ Owner — Limits search results to evidence owned by the user specified. To specify the user, click in the Owner box, start typing the name of the user, wait for the system to show the matching users, and then click the user you want. On the My Evidence page, the Owner filter is set to your name by default. □ Uploaded By — Limits search results to evidence uploaded by the user specified. To specify the user, click in the Uploaded By box, start typing the name of the user, wait for the system to show the matching users, and then click the user you want. □ 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. □ Tag — Limits search results to evidence whose tags includes the characters you enter in the Tag box. Evidence Map Search Feature - GPS tagging is available when one of TASER's free mobile applications, Axon View and Axon Capture, is installed on an officer's smart device and paired to his camera via Bluetooth.

Functional Category: CAMERA			
Reference Number	Business Requirements	Response Code	Comments
			The Axon will source GPS location information from the mobile device and video files are automatically tagged with GPS locations. When a new coordinate is received, the coordinates are sent to the camera system. The metadata is pulled directly from the smart device's GPS coordinates and the location is then geotagged in Evidence.com. If the FLPD's Records Management System or Computer-Aided Dispatch System is integrated with Evidence.com, GEO-tagging will be available using the address sourced from the RMS or CAD system. This integration effectively automates the process of tagging videos with complete, correct metadata. The Evidence Map feature shows pin icons for any evidence with associated location information and basic features for finding and viewing a location on the map. The map pin style used for an evidence file is determined by the category assigned to the evidence.

Functional Category: CAMERA			
Reference Number	Business Requirements	Response Code	Comments
CA-24	At a minimum software should be compatible with Microsoft Windows 7 64 bit.	**SF**	The only system requirement for using Evidence.com is a modern Web browser; therefore, Evidence.com can be used on any variety of operating systems. Unlike traditional systems with vast infrastructure requirements, Evidence.com requires only internet connectivity and can be accessed from any supported internet browser. There are there are no CPU or hardware requirements to run the application. Evidence.com leverages virtual computing and can scale resources quickly to handle increased demand. For example, when performing CPU intensive tasks such as redaction. This is, of course, opaque to the FLPD and all done automatically. **Evidence Sync Minimum System Requirements** -Windows XP or 7 -Microsoft Direct X (Version 7.0 or greater for exported incident video processing) -Adobe Reader -Apple QuickTime or VLC Media Player -Pentium 4 or AMD Athlon Processor -128 MB of RAM -Audio Card -Video Card (1024 x 768 Resolution or Better, with 24-bit Color) -PATA Hard Drive with At Least 2 GB of Available Disk Space -Internet Access (Recommended) -2.0 Self-Powered USE BUS or HUB

Functional Category: CAMERA

Reference Number	Business Requirements	Response Code	Comments
CA-25	Provide capability of requiring metadata entry by Officers after recording is stopped based on the following configurable settings by an Administrator: • Forced – after the officer stops the recording, they MUST select an option from a configurable list of values* • Enabled – after the officer stops the recording, gives the officer the option to select an option from a configurable list of values • Disabled – after the officer stops the recording, officer is not prompted to select an option from a configurable list of values	**SF**	Axon devices are designed as a sealed compartment with no moving parts, articulating heads or fragile electronics (LCD screens). Axon View, a free mobile application, automatically maps video files with GPS data when paired to a smart device with GPS capabilities. Officers can annotate the following metadata fields. Axon View transfers the tag information to the camera. □ ID –Case ID of incident □ Title –Titles default to the device type, date and time of the video capture “Axon Body 2 Video 2012-10-13 1447”. This field can be updated by the user at the time of capture to display a more specific title (i.e. suspect name or address of incident). □ Category –Allows searching for any category type or to specify any category added by the Agency (i.e. traffic violation or felony arrest). When an officer’s smart device is paired to an Axon camera via Bluetooth, Axon View pulls the pre-defined categories and retention criteria from the agency’s Evidence.com account. This limits the category assigned to a video or bulk group of videos to one category selection. When an officer places his or her camera in the Axon Dock, the videos stored on the camera automatically upload to Evidence.com with the tag information applied using Axon View.

Functional Category: CAMERA			
Reference Number	Business Requirements	Response Code	Comments
CA-26	Should be able to export video format and be compatible with the following: • MP4 • AVI • WMV • WAV • MOV • H.264 • MPEG • DIVX	**SF**	The Axon conforms to the MPEG-4 Part 2 video compression format, which utilizes a MP4 container and the H.264 compression standard. This format is non-proprietary and allows for playback from any general video player. A full list of the file types supported is listed on pages 120-121 of the Evidence.com Administrator Guide (Tab 10M).
CA-27	Should have the capability to control the volume for audio and visual playback in the vehicle.	**SF**	Playback of video stored on the device can be viewed using a smart device running the Axon Mobile application with a paired camera. Volume of playback will be controlled through the device.

ATTACHMENT A - FORT LAUDERDALE POLICE DEPARTMENT (FLPD) BODY WORN CAMERA AND DIGITAL EVIDENCE MANAGEMENT SYSTEM FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS

Vendor Response Codes

SF	Standard Function ("Out-of-the-Box")
NR	Provided in Next Release
MD	Modification
TP	Third Party Software Required
NA	Cannot Meet Requirement

(If any vendor response other than **SF**, or if you cannot meet or have an alternate solution please - INCLUDE COMMENTS IN "COMMENTS BOX"

Functional Category: Digital Evidence Management System

Reference Number	Business Requirements	Response Code	Comments
CS-1	Software Management should be capable of configuring/managing access control: • Retention management (auto purge) • Secure transport • Full audit trail on every action	**SF**	For proper management, agencies must create a set of agency-specific Categories large enough to properly segregate evidence by type for retention-setting and search functionality. Categories can be edited or added later within Evidence.com by users with appropriate access. The evidence retention policy determines: 1. Whether the system will initiate automatic deletion of evidence assigned to the category. 2. How long the system waits before initiating the deletion of evidence that is not included in a case. Axon video deletions are based on the recording date. Deletion of all other evidence is based on the upload date. **Secure Transport** Evidence.com uses strong encryption to protect evidence data in transit and at rest. Data in Transit - Evidence data is encrypted during transfer: SSL with RSA 2048 bit key, 256 bit ciphers, TLS 1.0-1.2, Perfect Forward Secrecy Data at Rest - Evidence data is encrypted in storage: 256-bit Advanced Encryption Standard (AES-256) **Audit Trails** Information access via Evidence.com is controlled through a robust "Access Control System" managed by the Administrator and that features comprehensive audit trails. Access to information is governed by the agency-defined access control system built into Evidence.com. Access is controlled according to: □ Pre-defined roles □ Pre-defined individuals (i.e., who has access to what data feed) □ User account-specific passwords

Functional Category: Digital Evidence Management System

Business Requirements			Comments
Reference Number		Response Code	
CS-2	Software management should provide Microsoft Active Directory integration with the cloud based hosted system. Please describe integration details and constraints.	SF	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, officers no longer need to juggle multiple usernames and passwords. With Active Directory federation, Evidence.com uses the agency's network to authenticate users. Agency credentials are never sent to Evidence.com. This means that if a user changes their password on Active Directory they will log in with that new password.
CS-3	At a minimum software should be compatible with Microsoft Windows 7 32/64 bit and current browsers. Please list browser compatibility.	SF	The only system requirement is a modern Web browser; therefore, Evidence.com can be used on any variety of operating systems. Unlike traditional systems with vast infrastructure requirements, Evidence.com requires only internet connectivity and can be accessed from any supported internet browser.
CS-4	Browser based solutions should be compatible with top used web browsers. List browser compatibility.	SF	TASER supports the use of Evidence.com with the following web browsers: □ Internet Explorer version 10 and above Note: If you use Internet Explorer, ensure that Compatibility View is disabled. Evidence.com does not support the use of the Compatibility View feature. To verify your Internet Explorer settings, go to Tools > Compatibility View settings and ensure that Evidence.com is not included in the list of websites added to Compatibility View and that the "Display all websites in Compatibility View" check box is cleared. □ Chrome version 40 and above □ Firefox version 30 and above □ Safari version 8 and above Additionally, TASER supports the media player and related tools, introduced in Evidence.com release 1.27, with the following web browsers: □ Internet Explorer version 10 and above □ Chrome version 43 and above □ Firefox version 38 and above □ Safari version 8 and above If you use an unsupported browser to access media-evidence files, Evidence.com provides the traditional media player. It is strongly recommended that you always use the latest release of Adobe Flash.

Functional Category: Digital Evidence Management System

	Business Requirements		Comments
Reference Number		Response Code	
CS-5	The system should allow multi-faceted role-based security levels for activities within the system. Example: (Division Assignment + Role = permission/access to video) System must facilitate security to segregate video and multi-media files by divisions and units.	SF	Each Evidence.com user is assigned a role. Roles determine a user permissions, which control levels of access to features and functions in Evidence.com. Information access via Evidence.com is controlled through a robust "Access Control System" managed by the Administrator and features comprehensive audit trails. Access to information is governed by the agency-defined access control system built into Evidence.com and is controlled according to: □ Pre-defined roles, □ Pre-defined individuals (i.e., who has access to what camera feed), □ User account-specific passwords. Administrators assign the roles and actions of all users and create individual user accounts with varying degrees of access, i.e. administrative accounts, basic user accounts, etc. Account administrators can customize the roles and authorization levels of each account user, or what they are permitted to do. This functionality was created to preserve chain of custody and to clarify what each user is permitted to do. Administrators can allow or prohibit a user access to specific features and functions depending on the level of access granted to the user(s). You can restrict access to the following functions, but this is not a complete list: □ Edit Account Information □ View & Compose User Messages □ Download Evidence Sync Software □ Configure IP Restrictions □ Edit Agency Settings □ Edit Device Offline & Microphone Settings □ Device Administration □ User Administration □ Category Administration □ Generate Reports □ User Search □ Evidence Search □ Device Search □ Case Search □ Upload External Files
CS-6	System should have the ability to enforce security by Active Directory (AD) group memberships.	SF	The Group feature provides additional control of which evidence can be viewed by users. This feature is fully configurable allowing the agencies to create groups that reflect the ranking system already in place. Creating groups and dictating their specific rights in the system is quick and intuitive. For example, with groups, an agency can grant unit leaders the ability to view the evidence of their team members only. The Group feature complements the Roles and Permissions feature. Unit leaders no longer must be granted permission to view all evidence of the agency, and this permission should be removed from leaders when an agency implements the Groups feature.

Functional Category: Digital Evidence Management System

Reference Number	Business Requirements	Response Code	Comments
CS-7	Encryption in transit should use SSL 1024 bit key or better and at rest AES 256 or better.	SF	Evidence.com uses strong encryption to protect Evidence data in transit and at rest. FIPS 140---2 approved encryption ciphers (or stronger) Robust SSL/TLS implementation for data in transit. RSA 2048 bit key TLS 1.2 with 256 bit connection Perfect Forward Secrecy 256 bit AES encryption for evidence data in storage
CS-8	Have the capability, at a minimum, to search by: • Name (last, first, middle) • Date and time video was recorded • Date and time video was uploaded • Date and time video was viewed • Event ID • Offense Case Number • Offense Type • Vehicle ID • Officer name • Officer ID Number • Geo Fence search • District/Squad • Wild cards	SF	By enabling officers to annotate Axon video with meta-data, Evidence.com turns what was once an overwhelming amount of files and information into a database of highly searchable evidence. **Text Search** For evidence searches, the ID, Title, and Tag filters provide advanced text matching features. ☐ The text you enter can match any part of the data you are filtering. For example, if you enter 21 in the ID box, any evidence whose ID includes “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. For example, if you enter 21 78 in the ID box, search results include evidence with the ID 213789 as well as 421278. ☐ The order of text strings is irrelevant. **Evidence Search Filters** 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 to narrow your results. ☐ All Evidence — Finds all evidence, including evidence that you do not have permission to view. ☐ My Evidence — Finds evidence that you own. Under Filter Evidence, the Owner filter is automatically set to your name. ☐ Shared Evidence — Finds evidence that has been shared with you by the evidence owner. **Evidence Search Fields** ☐ ID — Limits search results to evidence whose ID includes the characters you enter in the ID box. ☐ Title — Limits search results to evidence whose title includes the characters you enter in the Title box. ☐ Category — Limits search results to evidence that is assigned to the category that you select. By default, search results include evidence assigned to any category, including uncategorized evidence. ☐ Date — Limits search results by either the recorded, uploaded, or deletion date of evidence, as selected. You must also specify a date range by using the From and To boxes, else the search is not limited by date range. Search results are inclusive of the dates specified. o From — The start of the date range. If the From box is empty, the date range begins with the earliest possible date. o To — The end of the date range. If the To box is empty, the date range ends with today. ☐ File Type — Limits search results to the file type selected. By default, search results include all file types.

Functional Category: Digital Evidence Management System

	Business Requirements		Comments
Reference Number		Response Code	
CS-8			□ Owner — Limits search results to evidence owned by the user specified. To specify the user, click in the Owner box, start typing the name of the user, wait for the system to show the matching users, and then click the user you want. On the My Evidence page, the Owner filter is set to your name by default. □ Uploaded By — Limits search results to evidence uploaded by the user specified. To specify the user, click in the Uploaded By box, start typing the name of the user, wait for the system to show the matching users, and then click the user you want. □ 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. □ Tag — Limits search results to evidence whose tags includes the characters you enter in the Tag box. □ Group — Limits search results to evidence owned by members of the group specified. To specify the group, click in the Group box, start typing the name of the group, wait for the system to show the matching groups, and then click the group you want. □ Flagged — Limits search results to evidence whose flag status matches the flag status selected. **Evidence Map Search Feature** GPS tagging is available when one of TASER's free mobile applications, Axon View and Axon Capture, is installed on an officer's smart device and paired to his camera via Bluetooth. The Axon will source GPS location information from the mobile device and video files are automatically tagged with GPS locations. When a new coordinate is received, the coordinates are sent to the camera system. The metadata is pulled directly from the smart device's GPS coordinates and the location is then geotagged in Evidence.com. If the FLPD's Records Management System or Computer-Aided Dispatch System is integrated with Evidence.com, GEO-tagging will be available using the address sourced from the RMS or CAD system. This integration effectively automates the process of tagging videos with complete, correct metadata. The Evidence Map feature shows pin icons for any evidence with associated location information and basic features for finding and viewing a location on the map. The map pin style used for an evidence file is determined by the category assigned to the evidence.
CS-9	Have the ability to upload/intake/receive video/multimedia files from multiple users simultaneously from multiple geographic locations.	**SF**	Evidence.com is a cloud-hosted digital evidence management solution provided as a service (SaaS) application. It is horizontally scalable and can elastically adapt to accommodate any traffic volumes. Internally, the solution uses a service oriented architecture where functionality is provided by discrete compassable services that can run on one or many servers. This allows individual components to scale to handle changes in traffic volumes. The application is designed to support uploads from multiple users, devices, and locations, simultaneously from thousands of agencies across the United States. It is also possible for concurrent users to access the same video at the same time.

Functional Category: Digital Evidence Management System

Reference Number	Business Requirements	Response Code	Comments
CS-10	Have an audit trail generated for every video and/or mulitimedia file: • Viewing • Tagging • Upload • Historical after purge • Trails based on date and time • Usernames and/or ID numbers • File access • Exporting of files • File security changes • System settings changes • Extend to external sharing	SF	The User Audit Trail shows many of the actions taken by a user in addition to changes to the user's account. It does not show activities related to devices, evidence, or cases. The Evidence.com auditing functionality provides the source IP Address of all actions. Location can be associated with uploaded content, and can be viewed on Evidence.com. In addition to evidence-related user actions, the User Audit Trail provides the following information: □ Failed login attempts will be entered into the user's individual audit trail and show the IP address. □ When a user is locked out of their account due to multiple failed login attempts the user's audit trail will show the IP address of the computer that attempted logging in. □ When a user's password has been reset or their account has been unlocked the audit trail will show the username, first and last name, and badge ID of user who has taken that respective action. 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 □ Extend evidence retention period □ 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
CS-11	ystem should allow redaction of video and/or audio by administrator role or appropriate security role. Edited versions shall disclose they are not the original version. Original version shall be retained and unaltered.	SF	Evidence.com features a full redaction suite natively within the application. This functionality is available to all licensed users, subject to your agency's role-based access controls. Evidence.com offers both automated and manual options for redacting an evidence file (or multiple evidence files). Evidence.com offers users three options to redact videos, each to be used in a different scenario: Bulk Redaction, Smart Tracker Redaction and Manual Redaction. Both Bulk and Smart Tracker Redaction options are automated. Each of these options are simple and easy to use, allowing the FLPD personnel to manage public information requests quickly. The automatically generated title of a redacted video or clip contains both the original name and the word "redacted".

Functional Category: Digital Evidence Management System

Reference Number	Business Requirements	Response Code	Comments
CS-12	Original version shall be retained and unaltered.	**SF**	To ensure a robust chain of custody, evidence can be verified for authenticity by matching the SHA hash of original file ingested in Evidence.com with the copy. The original data associated with a video is never changed. All modifications are handled by creating new, derivative files. Detailed audit logs track all evidence access. The best way to describe how Evidence.com manages video is through layers. The two bottom layers are the original video and audio. Those two layers are never tampered with or manipulated. When we apply markers, clips, or redaction they exist in layers above the original content. The best way to imagine this would be to picture a translucent sheet over a picture or painting. Editing is simply drawing on the sheet, and then removing the sheet. This leaves you with an un-altered original image. When a user applies redaction to a video, all of their actions are saved to an XML file, much like the translucent sheet. When the video is played back the sheet is layered back over the video. Even when a redacted video is exported from Evidence.com, the video is created (encoded) on the fly and saved to the local hard drive.
CS-13	Be able to perform redaction on: • video track • audio track • perform privacy masking Redaction activities can be completed independently or in combination with one another.	**SF**	**Please see the Detailed Redaction Overview and pages 132 - 147 of the Evidence.com Administrator Guide, included as appedices.** offers users three options to redact videos, each to be used in a different scenario: Bulk Redaction, Smart Tracker Redaction and Manual Redaction. Both Bulk and Smart Tracker Redaction options are automated. Each of these options are simple and easy to use, allowing the FLPD personnel to manage public information requests quickly. **Bulk Redaction -** To aid with large public disclosure requests, the Bulk Redaction feature allows a user to queue video evidence for bulk redaction. Bulk redaction creates a copy of the original video and a blur filter over the entire video automatically. It can also remove audio for the duration of that copy. 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. **Smart Tracker Redaction -** Smart Tracker Technology within Evidence.com brings intelligent, automated support to agency video redaction workload. Using the Smart Tracker technology, users can easily create a redaction that tracks up to 10 objects in a video. For each object, specify a start and end frame. On each start frame, place and size a redaction mask. Once a user is done preparing assisted redaction, Evidence.com's technology tracks the redacted objects automatically and sends a notification email when it has finished creating the redaction. It is recommended that users closely verify redacted clips created using assisted redaction. If corrections are necessary, Evidence.com allows for manual edits to redacted clips. **Manual Redaction Concepts -** Manual redaction allows the user to control size, shape, and placement of redaction masks precisely, frame by frame. Creating a redaction manually involves working with several important concepts. □ Object—Organizes the mask segments that redact one actual object in the video. A redaction contains one or more objects. An object contains one or more mask timelines. □ Mask—Defines a rectangular area in a continuous segment of video frames that are redacted. A mask has three dimensions: o Height, defined by the mask frame o Width, defined by the mask frame o Duration, defined by the start and end handles of the mask segment. □ 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. □ Mask Frame Handle—Enables you to change the size and shape of the mask frame.

Functional Category: Digital Evidence Management System

Reference Number	Business Requirements	Response Code	Comments
CS-14	Redaction activities can be completed independently or in combination with one another.	**SF**	Users can apply multiple redaction actions to a single piece of evidence using Evidence.com's robust redaction suite. Please see Tab 10L for detailed information on the Evidence.com redaction suite.
CS-15	Redaction should require minimal human intervention and not require frame by frame human action. It shall make maximum use of automated face detection etc. Please describe in detail the redaction capabilities.	**SF**	Evidence.com provides the ability to redact video evidence files as needed, such as to protect the identity of persons in a video. The redaction tools enable you to create redacted versions of video evidence files without affecting the original file. In Evidence.com, a redaction is a set of information that tells Evidence.com; what to redact in a video. When you have completed creating or editing a redaction, you can extract a redacted video. 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. 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, Evidence.com tracks the redacted objects automatically and 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. 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. Please see Tab 10L for detailed information on the Evidence.com redaction and pages 132 - 147 of Tab 10M, the Evidence.com Administrator Guide.

Functional Category: Digital Evidence Management System

Reference Number	Business Requirements	Response Code	Comments
CS-16	System should contain a security administrator role to control user permissions/roles in the system including, but not limited to: • Search functions • Renaming • Redaction • Deletion • Copy • Download/upload • External agency sharing	SF	Each Evidence.com user is assigned a role. Roles determine a user permissions, which control levels of access to features and functions in Evidence.com. Information access via Evidence.com is controlled through a robust "Access Control System" managed by the Administrator and features comprehensive audit trails. Access to information is governed by the agency-defined access control system built into Evidence.com. Access is controlled according to: □ Pre-defined roles, □ Pre-defined individuals (i.e., who has access to what camera feed), □ User account-specific passwords. Administrators assign the roles and actions of all users and create individual user accounts with varying degrees of access, i.e. administrative accounts, basic user accounts, etc. Account administrators can customize the roles and authorization levels of each account user, or what they are permitted to do. This functionality was created to preserve chain of custody and to clarify what each user is permitted to do. Administrators can allow or prohibit a user access to specific features and functions depending on the level of access granted to the user(s). You can restrict access to the following functions, but this is not a complete list: □ Searching □ Editing Titles / IDs □ Download Evidence Sync Software □ Redaction □ Download Files □ Sharing files (interanally or externally) □ Device Administration □ User Administration □ Category Administration □ Generate Reports □ User Search □ Evidence Search □ Device Search □ Case Search □ Upload External Files
CS-17	If application is installed on the user’s PC, it shall contain methods of security to prevent unauthorized access.	SF	Not applicable. Users can access Evidence.com, TASER’s web-based evidence management interface, from any supported internet browser. This is a standard feature of Evidence.com, so requires no configuration.

Functional Category: Digital Evidence Management System

	Business Requirements		Comments
Reference Number		Response Code	
CS-18	Allow the user to run application after initial installation without local administrative access to users PC, including software updates.	SF	Not applicable. Users can access Evidence.com, TASER's web-based evidence management interface, from any supported internet browser. This is a standard feature of Evidence.com, so requires no configuration. TASER releases software patches on both a scheduled and nonscheduled basis as required. Updates to firmware supporting Axon cameras and Axon Docks are "pushed" from the internet to the local devices though the Axon Docks without the need for Agency interaction. Evidence.com software upgrades are handled in a similar way. TASER will release a software update to Evidence.com during a period of low traffic usage. Software upgrades are "pushed" to Evidence.com and are immediately available to you as soon as you log on, eliminating the need to perform manual software updates. The Evidence.com operations team at TASER applies these upgrades remotely, eliminating any worries about properly integrating or updating your systems. The latest product features and enhancements are included as part of your investment in Evidence.com. Evidence.com software is updated regularly throughout the year, and these updates are included in the price of your software licenses. TASER releases software patches on both scheduled and nonscheduled basis as required. Patches contain fixes to known issues reported by internal resources or by users at police agencies. There are no additional costs for any software patch or fix deployed. Patch deployment involves minimal or no downtime for the customer's solution. Scheduled maintenance will take place according to our monthly routine maintenance schedule. Routine maintenance is currently scheduled on the fourth Tuesday of each month from 7:00 PM to 8:00 PM Pacific Time. When possible, you will be informed one week prior to any changes to the maintenance schedule. Software updates, patches and fixes are included in the purchase of Evidence.com licenses. Release Notes and Documentation A detailed email is sent to system administrators when new releases, updates or upgrades are made to Evidence.com, Evidence Sync or Axon hardware. The Release Notes page in Evidence.com displays links to the release notes containing a summary of features and enhancements for the current and previous releases. The User Guides page displays links to guides that provide detailed information on Evidence.com features. Release notes and user guides are in PDF format. As updates and features are released, your Regional Support Manager will troubleshoot all changes to ensure a successful experience for customers.
CS-19	Vendor shall provide litigation and expert testimony in court if needed. Please provide details regarding availability and cost, if any.	SF	TASER employs experts in technology and information security, who can testify in court for the FLPD. TASER will send an employed expert to testify in court matters free of expert fee charges (capped at 100 hours per year and excluding reasonable travel expenses) in relation to the Evidence.com product lines regarding data security and chain of custody matters. FLPD must provide TASER with reasonable notice, in no event less than five business days. If FLPD requires more than 100 hours per year during the term of the Contract, an hourly rate will be negotiated by the parties and travel expenses will be reimbursed by FLPD at GSA per diem rates. Anything outside the scope of the expert testimony described above is subject to the attached expert witness terms and conditions and fee schedule. Anything outside the scope of this expert testimony is subject to the attached Expert Witness Terms and Conditions and Fee Schedule, in Tab 8b.

Functional Category: Digital Evidence Management System

	Business Requirements		Comments
Reference Number		Response Code	
CS-20	Should be able to import other digital audio, video, and photos into the DEMS to use with BWC data to create case files. Explain this feature and any limitations.	**SF**	Evidence.com provides law enforcement with a robust solution for organizing, classifying, managing, viewing, and archiving all of their digital evidence – not just Axon videos. Evidence.com provides law enforcement with a robust solution for organizing, classifying, managing, viewing, and archiving all of their digital evidence – not just Axon videos. 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 □ Audio: MP3, WAV Documents and non-supported digital media types can be uploaded and managed in Evidence.com; however, online preview features are not available for unsupported file types. These file types are typically proprietary formats that require custom players. A full list of the file types supported is listed on pages 120-121 of the Evidence.com Administrator Guide (Tab 10M).

Functional Category: Digital Evidence Management System

	Business Requirements		Comments
Reference Number		Response Code	
CS-21	Allow sharing video and/or case files (including non-BWC files) with the State Attorney's Office and other agencies with options for viewing, burning, sharing, set custom access time length, restrict viewing to only once, restrict burning to only once, etc. Fully explain this feature and any limitations.	**SF**	There are several options for sharing evidence with interested parties. Internal Sharing allows for intra-agency sharing of evidence, ideally from an officer to a superior. When an officer wishes to share the video, they simply select the share option adjacent to their video, and then enter the First or last name, or the badge number of their superior. External sharing allows for inter-agency sharing, or sharing with organizations like City and District Attorneys. In the same way an officer can share a video with a superior, an employee with Administrative rights on Evidence.com can share a video outside of the Agency. This is particularly useful for FOIA requests and public records requests. The collaboration function is focused on the inter-agency aspect of sharing. If two agencies choose to collaborate, they no longer have to enter an entire e-mail address, as they would normally when externally sharing. If your Administrator wanted to share a video with another Agency, rather than specifying the recipient’s email address, they would simply be able to type in their name. The feature is at the discretion of the Agency administrator. And agencies that you collaborate with do not have visibility to your Agency’s content. It’s simply designed to make sharing a bit easier. When all of the evidence pertaining to an incident has been grouped together in a Case, you can transfer that package to your trusted Partner Agencies. When they accept the case, they will have their own copy of the files to manage independently. They can then control their own retention policies and access rights without affecting yours. Another option is to create an account for the external party that is highly restricted only to videos that are shared with them by the Agency. The Agency can also assign a time limit, limiting the external parties’ ability to watch the video to a specified amount of days. A User can also access a file on Evidence.com, download the file, and then burn or copy the file to CD, DVD or a flash/USB drive. Bulk Share by Unauthenticated Download Link - Bulk sharing enables the agency to share more than one evidence file at a time. Sharing by download link makes the shared evidence available through a web link, or URL, for downloading a ZIP file of the evidence from Evidence.com—without requiring the person downloading the evidence to sign in to Evidence.com. Bulk Share Evidence by Authenticated Sharing - Bulk sharing enables the agency to share more than one evidence file at a time. Authenticated sharing enables you to share evidence with other users of Evidence.com. The agency should use authenticated sharing when it is required that evidence is available only to users who sign in to Evidence.com. The agency can control whether users with whom evidence is shared can view the evidence, download the evidence, view the audit trail of evidence, and share the evidence with others. Bulk sharing evidence grants each user the same permissions to the shared evidence. If the agency needs to grant different permissions to different users, this procedure is performed once for each set of users granted the same permissions. These permissions can be revoked at any time based on a certain time limit the agency sets or through a manual revoking of the permissions granted.

Functional Category: Digital Evidence Management System

Reference Number	Business Requirements	Response Code	Comments
CS-21	Allow sharing video and/or case files (including non-BWC files) with the State Attorney's Office and other agencies with options for viewing, burning, sharing, set custom access time length, restrict viewing to only once, restrict burning to only once, etc. Fully explain this feature and any limitations.	SF	Receiving Shared Cases from Partner Agencies The FLPD can enable a group to receive cases shared by partner agencies. When a partner agency shares a case, they can send it to groups permitted to receive shared cases. All members of the group receive a message notifying them of the invitation to receive the shared evidence. The user who accepts the case shared with the group becomes the owner of the evidence. While accepting the case, the user can add or remove evidence access for other group members. A group that is monitoring a group that receives a shared case from a partner agency can view the evidence of the shared case. External and Interagency Sharing Evidence.com makes it easy to send evidence to organizations like City and District Attorneys. Users can share a single file, multiple files, or, when all of the evidence pertaining to an incident has been grouped together in a case, a copy of the case and its evidence can be sent to trusted Partner Agencies. When they accept the case, the system creates a copy of the files, which they can manage independent of the original case and evidence. Likewise, they can then control their own retention policies and access rights without affecting any agency's evidence. Collaborating with another Evidence.com agency makes sharing evidence with that agency as simple as if they were part of your own agency, while still maintaining the agency's data security. Collaborating agencies have access only to that data specifically share with them. All unshared data belonging to an agency will remain unavailable to partner agencies. Evidence.com for Prosecutors - The same end-to-end evidence management solutions of Evidence.com now allow prosecutors to manage evidence of any type, from any agency, all in one place. Files can be shared during discovery, complete chain of custody is maintained, and all evidence is encrypted. Prosecuting attorneys working with agencies already using Evidence.com, standard licenses are provided at no cost.
CS-22	Allow remote viewing of stored files to field personnel via web based interface or application available for use on in-car Mobile Data Computers or smart device.	SF	Using the Axon View app, an officer can pair the Axon camera with his or her smart device via Bluetooth and review videos stored on the camera. Data is not stored on the smart device, and the officer cannot delete, alter or edit the videos. Using Axon View, officers can annotate the following three metadata fields: ID (i.e. incident number from CAD or RMS), Title (i.e. suspect name or address of incident), and Category (i.e. traffic violation or felony arrest). Alternatively, using Evidence Sync, TASER's Microsoft Windows application, the Axon camera can be connected to an in-car MDT or MDC via USB cable. Features are similar to Axon View, except that when video are played back over Axon View, they are played at 5 frames per second, Evidence Sync will playback video at the source frame rate of 30 frames per second. Using Evidence Sync from a MDT or MDC, officers can view files already uploaded to Evidence.com, with an internet connection.

Functional Category: Digital Evidence Management System

	Business Requirements		Comments
Reference Number		Response Code	
CS-23	Have full reporting capabilities for standard parameters as well as the ability to create custom reports as directed by FLPD staff. Please describe how custom reports are developed and provided.	SF	Evidence.com allows administrators and those with the reporting permission to generate reports showing Evidence.com utilization. These options can help your agency turn that data into valuable answers to ensure your Evidence.com account is providing you with the flexibility and utility your agency deserves. Evidence.com has pre-set categories; however, agencies can add customized categories based on Agency guidelines and protocols. Report Types □ 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. □ Evidence Deleted — Lists all evidence deleted and associated metadata on your agency's account in order of when the data was deleted. This report will give better monitoring of automated deletions and help ensure a proper retention policy is in place. □ Category Summary — Lists the current count of total files and file size in megabytes (MB) for each category as well as the percent of files assigned to that category. □Uncategorized Evidence – Lists users with uncategorized evidence assigned to them. A second tab on the export lists every piece of uncategorized evidence and includes the owner information, evidence title, date recorded, and link to the evidence. □ User Summary — Lists total files and file size in MB, broken out by owner of the evidence. The counts are further broken out by evidence type, active, and deleted evidence. □ 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 uploads by the specified grouping: Day, Month, or Year. □ Sharing Audit Report — The Sharing Audit report exports a list of all user actions related to sharing evidence and cases to a CSV file. You can specify the date range for the report. 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. You can download reports either by visiting the Reports page or by the download link in a notification email. Completed reports are available from the Download Queue section of the Reports page. If you have permission to run reports, you can download reports that any user has run. Evidence.com reports are spreadsheets in an XLSX file format, which 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 of time.

ATTACHMENT A - FORT LAUDERDALE POLICE DEPARTMENT (FLPD) BODY WORN CAMERA AND DIGITAL EVIDENCE MANAGEMENT SYSTEM FUNCTIONAL AND NON-FUNCTIONAL REQUIREMENTS

Vendor Response Codes

SF	Standard Function ("Out-of-the-Box")
NR	Provided in Next Release
MD	Modification
TP	Third Party Software Required
NA	Cannot Meet Requirement

(If any vendor response other than **SF**, or if you cannot meet or have an alternate solution please - INCLUDE COMMENTS IN "COMMENTS BOX" BELOW)

Functional Category: CLOUD STORAGE

Reference Number	Business Requirements	Response Code	Comments
CS-1	Web-based can host digital evidence management, storage, and retrieval system.	**SF**	Users can access Evidence.com, TASER's web-based evidence management interface, from any supported internet browser. This is a standard feature of Evidence.com, so requires no configuration.

Functional Category: CLOUD STORAGE

Reference Number	Business Requirements	Response Code	Comments
CS-2	CJIS compliant security of data during connection and transfer to hosted cloud solution minimum of 256-bit AES encryption using SHA-1 algorithm. Encryption in transit should use SSL 1024 bit key or better and at least AES 256 or better.	**SF**	Evidence.com uses strong encryption to protect evidence data in transit and at rest. Data Protection □ Data in Transit - Evidence data is encrypted during transfer: SSL with RSA 2048 bit key, 256 bit ciphers, TLS 1.0-1.2, Perfect Forward Secrecy □ Data at Rest - Evidence data is encrypted in storage: 256-bit Advanced Encryption Standard (AES-256) All communication to and from Evidence.com is conducted via 256-bit AES encryption. □ At the time the camera(s) are connected to the docking station they are recognized and analyzed. □ Part of the analysis is to apply the SHA cryptographic hash function. A SHA checksum is generated for every MP4 video on the Axon camera. In layman's terms the DNA of each video file is captured. □ The cryptographic hash function and various annotations the officer has entered pertaining to the video are transmitted to Evidence.com. Upon receipt the upload process begins. □ At the completion of the upload process, the SHA cryptographic hash values are evaluated to detect data corruption of any kind. □ Once the upload is completed and the data integrity verified, the camera information is deleted. □ The MP4 file now saved on Evidence.com in all essence is the original copy down to the last bit, as verified by the SHA.

Functional Category: CLOUD STORAGE

Reference Number	Business Requirements	Response Code	Comments
			□ The MP4 file now saved on Evidence.com in all essence is the original copy down to the last bit, as verified by the SHA. TASER deploys a comprehensive Information Security Program (ISP) to provide for the confidentiality, integrity and availability of all customer data in Evidence.com. Security is integrated throughout TASER International's products, development processes and corporate culture to ensure the security of data and maintain trust with customers. Our security program includes frequent penetration tests, static code analysis, white box testing, and designing of solutions that provide PKI-based end-to-end encryption with digital authenticity and integrity signing. The Evidence.com Information Security program is compliant with the defined requirements of ISO/IEC 17021:2011 and ISO/IEC 27001:2013, and is rigorously reviewed and audited to ensure compliance with the CJIS Security Policy.
CS-3	Should have environmental safeguards of data centers such as: • Fire detection and suppression • Uninterruptible power supplies • Power generator management • Climate control	**SF**	Within the data centers that host Evidence.com, environmental controls such as fire detection and suppression systems, air conditioning and humidity monitoring systems, uninterruptible power supply (UPS) units, and generators are in place to protect assets.

Functional Category: CLOUD STORAGE

Reference Number	Business Requirements	Response Code	Comments
CS-4	Security of hosted network gateways using Intrusion Detection and Prevention, restrictive firewall rule sets.	**SF**	Evidence.com uses intrusion detection/prevention solutions and restrictive networking rules to as part of a holistic approach to securing the application. Evidence.com employs advanced detection and analysis capabilities of system events. This includes automated detection and alerts for unusual activity or attacks. TASER International maintains a robust information security program designed to provide a high level of protection against current and emerging threats. This includes logging all access to evidence data and systems, and robust audit reports within Evidence.com. The Evidence.com infrastructure utilizes a multi-tier design that segregates the database tier from web and application tiers using firewalls and network ACLs. Evidence.com utilizes host-based firewalls on all applicable systems. Host based IDS and AV are deployed on applicable systems.

Functional Category: CLOUD STORAGE

Reference Number	Business Requirements	Response Code	Comments
CS-5	Redundancy of network gateways using multiple, physically non-contiguous US locations in case of network related issues of host server.	**SF**	The Axon solution will provide maximum security against data loss using industry best practices and minimize, if not eliminate any possible interruption to service: □ Multiple Locations - Each Evidence.com region is comprised of multiple, isolated locations and all Evidence.com application components are duplicated across all these locations for a fully redundant, Hot/Hot failover, infrastructure □ Highly Available - Evidence.com is spread across isolated locations, and all components (e.g. databases, web servers) are further backed up daily to a highly available and durable storage location to support a Hot/Cold failover and recovery objective. □ Automatic Failover - No human intervention is required in the event of a primary data center failure. □ Active-Active Topology - Because the solution was designed from the start to run as a highly-available application, it is equipped to handle a wide range of failures in the underlying infrastructure. The active-active design means that computing resources are efficiently utilized, no resources are wasted on “standby” servers. □ Commodity Hardware - No special systems required for high-availability. □ Local Replication –the application also makes its easy, should the FLPD wish, to keep local copies of certain content. The application provides “Bulk Download” functionality.

Functional Category: CLOUD STORAGE

Reference Number	Business Requirements	Response Code	Comments
CS-6	Have third party vendor access to system prohibited unless allowed by authorized personnel at the Fort Lauderdale Police Department.	**SF**	TASER employees do not have access to a customer's evidence data without the explicit authorization from the customer. The only exception to this is for a small team of administrators who would only access evidence data in the event of a system emergency. In order to gain access to evidence data, the administration team is authenticated by at least two factors (username/password, and a time-based security token). Such access is closely logged, monitored and correlated to appropriate business need by the TASER Information Security team. All TASER personnel that may encounter customer evidence data as part of their job responsibilities are subject to the appropriate local adjudication processes. Evidence data access is also logged and closely monitored. Those events are captured in the audit log for that piece of evidence. TASER does not have persistent access in the application to those logs but do have a group of system administrators that have access to the database that stores the logs.
CS-7	Options preferred for Two Factor Authentication, IP access restriction/filtering, and/or security challenge questions upon access from an unknown or previously used location.	**SF**	Evidence.com includes many security features that can be tailored by customers including: □ Mandatory challenge questions when authenticating from new locations □ Multi-factor authentication options for user login and prior to administrative actions (one time code via SMS or phone call-back) □ Role-based permission management □ Device-level permission management (for example, allow specific users to use the web-based interface, but not the mobile application) □ Restricted access to defined IP ranges (limit access to approved office locations)

Functional Category: CLOUD STORAGE

Reference Number	Business Requirements	Response Code	Comments
CS-8	System shall send email alerts when it is down, going down for maintenance, off-line, or any other alert pertaining to operational/security events.	**SF**	Scheduled maintenance will take place according to our monthly routine maintenance schedule. Routine maintenance is currently scheduled on the fourth Tuesday of each month from 7:00 PM to 8:00 PM Pacific Time. When possible, you will be informed one week prior to any changes to the maintenance schedule. Evidence.com employs advanced detection and analysis capabilities of system events. This includes automated detection and alerts for unusual activity or attacks. TASER International maintains security incident response procedures and capabilities for Evidence.com including prompt reporting to appropriate parties. Specific security event and incident handling practices have been implemented to ensure appropriate detection, analysis, containment, eradication and recovery in the event of an incident. If an incident is determined or reasonably believed to have impacted the security of customer data, then FLPD will be notified within an appropriate timeframe, typically within 48 hours of incident determination. The notification will reasonably explain known facts, actions that have been taken, and make commitments regarding subsequent updates. Additionally, TASER agrees to notify FLPD if there are changes to the threat environment or existing safeguards that would have a significant impact on the security, integrity or confidentiality of FLPD data.

Functional Category: CLOUD STORAGE

Reference Number	Business Requirements	Response Code	Comments
CS-9	Shall present full security methodology, network infrastructure, security protocols, physical and application layer security efforts to the FLPD Security Officer for review and approval.	**SF**	Security Compliance Certification TASER deploys a comprehensive Information Security Program (ISP) to provide for the confidentiality, integrity and availability of all customer data in Evidence.com. Security is integrated throughout TASER International's products, development processes and corporate culture to ensure the security of data and maintain trust with customers. Our security program includes frequent penetration tests, static code analysis, white box testing, and designing of solutions that provide PKI-based end-to-end encryption with digital authenticity and integrity signing. The Evidence.com Information Security program is compliant with the defined requirements of ISO/IEC 17021:2011 and ISO/IEC 27001:2013, and is rigorously reviewed and audited to ensure compliance with the CJIS Security Policy. Evidence.com will allow the FLPD to configure granular role-based access controls to ensure only authorized individuals can view and perform authorized actions on FLPD data. Evidence.com supports customer single sign-in (SSO) and account registration over Security Assertion Markup Language (SAML) to enable integration into existing FLPD identity services.

Functional Category: CLOUD STORAGE

Reference Number	Business Requirements	Response Code	Comments
			Additionally, Evidence.com provides many security features and capabilities to enable customers to secure digital evidence including password complexity requirements, failed login limits, and enforced timeout settings. Multi-factor authentication (MFA) options are also configurable for user login and prior to administrative actions. MFA can use a one-time code via SMS or phone call-back to provided phone numbers. Evidence.com requires two-factor authentication for all system administration access and many has features to provide robust access control. Administration is performed over a secured VPN connection. Passwords for system and application administration requires nine character passwords and contain at least three of the four character categories (Upper letter, Lower letter, Number, Symbol). Step-up authentication is performed using a one-time, 6-character code delivered out-of-band to a previously authenticated device. Evidence.com safeguards the integrity and authenticity of digital evidence. Features ensure evidence meets chain-of-custody requirements and authenticity can be proven to be authentic and free from tampering in the following ways: □ Forensic fingerprint of each evidence file using industry standard SHA hash function. Integrity is validated before and after upload to ensure no changes occurred during transmission.

Functional Category: CLOUD STORAGE

Reference Number	Business Requirements	Response Code	Comments
			□ Full tamper-proof audit records are created in real-time and available for FLPD review and monitoring. The evidence logs capture the when, who and what for each evidence file. These records cannot be edited or changed, even by account administrators. □ Original evidence files are never altered; even when derivative works (video segments) are created. □ Deletion protection, including deletion approval workflows, deletions notification emails, and a deletion remorse period to recover accidently deleted evidence files. Access to Client Data All customer access to data is controlled at layer 7 of the OSI model within the web application interface over HTTPS. Additionally, Evidence.com enables FLPD to control access at layer 4 of the OSI model by establishing IP whitelisting to define and limit the IP ranges in which an FLPD user may access Evidence.com. TASER International also protects Evidence.com at layer 4 by blacklisting known malicious IP addresses. TASER International protects and controls access on behalf of all Evidence.com customers at layer 3 of the OSI model. Customer data is uniquely identified and marked to ensure appropriate segregation of customer data. To protect the web application, TASER International deploys a web application firewall (WAF) to actively protect against threats in real-time.

Functional Category: CLOUD STORAGE

Reference Number	Business Requirements	Response Code	Comments
			Additionally, TASER International performs at least quarterly penetration testing of Evidence.com. Penetration testing includes testing to ensure customer data segregation is maintained and not commingled. Encryption All evidence data is encrypted at rest and in transit. Robust SSL/TLS is implemented for data in transit using TLS 1.2 with a 256 bit connection and Perfect Forward Secrecy. Evidence data stored at rest is encrypted with at least 256 bit AES. Disaster Recovery and Continuity Plan TASER has designed Evidence.com to be highly scalable and extremely resilient. Evidence.com customer data is stored within data centers located in Boydton, VA and Des Moines, IA. Each data center offers world-class security and system protection. All data centers employ backup power, climate control, alarms, and seismic bracing. In the event of a disaster, the system will failover automatically to the secondary site and provide uninterrupted service to customers, providing uninterrupted access during disaster events.

Functional Category: CLOUD STORAGE

Reference Number	Business Requirements	Response Code	Comments
			TASER maintains a Business Continuity Plan that encompasses Evidence.com operations and resiliency capabilities. This plan is reviewed periodically and is ISO 27001certified. Design, development and maintenance of Evidence.com is performed by TASER personnel within authorized facilities. These facilities are included in scope TASER's International Information Security Program. Design, development and maintenance are only performed in the United States. FLPD data stored within Evidence.com will remain in the United States. TASER has developed and operates secure software development lifecycle procedures (SDLC). Execution within the SDLC ensures security is evaluated at every phase of development and that quality measures are met. TASER does not outsource the development of Evidence.com and development resources are assigned and dedicated to the on-going development, quality and security of the product. CJIS Compliance TASER acknowledges and abides by all aspects of the CJIS Security Addendum, and we are contractually committed to meeting CJIS, as the CJIS Security Addendum is included by reference into the Evidence.com Master Services Agreement.

Functional Category: CLOUD STORAGE

Reference Number	Business Requirements	Response Code	Comments
			All TASER CJIS-authorized personnel are required to complete CJIS security training in compliance with the CJIS Security Policy. TASER uses 'CJIS Online' from Peak Performance Solutions to conduct and coordinate CJIS-specific security training. TASER personnel training records are available to customers within the CJIS Online system. Any additional FLPD-specific security awareness training can be conducted as required. In addition to security awareness, training, TASER CJIS-authorized personnel have undergone state and federal fingerprint based checks in certain states. TASER is prepared to coordinate with FLPD to ensure that all TASER CJIS-authorized personnel undergo checks in alignment with the requirements of the FLPD. TASER's CJIS compliance status has been validated independently by CJIS ACE and the underlying security program is audited on at least an annual basis by an additional third party as part of TASER's ISO 27001program. Risk Detection Evidence.com employs advanced detection and analysis capabilities of system events. This includes automated detection and alerts for unusual activity or attacks.

Functional Category: CLOUD STORAGE

Reference Number	Business Requirements	Response Code	Comments
			TASER International maintains a robust information security program designed to provide a high level of protection against current and emerging threats. This includes logging all access to evidence data and systems, and robust evidence audit reports within Evidence.com. The Evidence.com infrastructure utilizes a multi-tier design that segregates the database tier from web and application tiers using firewalls and network ACLs. Evidence.com utilizes host-based firewalls on all applicable systems. Host based IDS & AV are deployed on applicable systems.

SUPPLEMENTAL INFORMATION

Table of Contents

AXON Body 2

UNLIMITED HD.
NO DISTRACTIONS.

AXON BODY 2

A powerful platform
behind a simple camera

BEYOND A CAMERA AND BEYOND COMPARE

The #1 Video Platform | Unlimited HD | Constant Upgrades

Axon Body 2 takes the powerful simplicity of its predecessor to the next level. The single-unit design is now equipped with even greater capabilities like unlimited HD video, Wi-Fi video offload and industry-leading security enhancements. It's still part of the same growing platform that connects cloud, mobile and wearable technologies to give you a true end-to-end solution.

800-978-2737 axon.io/body2

AXON BODY 2
FEATURES AND BENEFITS

RETINA HD VIDEO: The industry's best low-light video now records in HD.

FULL-SHIFT BATTERY: 12+ hours

PRE-EVENT BUFFER: Capture up to 2 minutes before an event.

WIRELESS ACTIVATION: Axon Signal turns the camera on with lightbar and other sensor activation.

WI-FI VIDEO OFFLOAD: Axon Body 2 is capable of wireless offload to the cloud.

OPTIONAL MUTE: Ability to disable audio in the field to support dual party consent.

IN-FIELD TAGGING: Add a marker to important points in your video.

UNMATCHED DURABILITY: Built to withstand extreme weather and brutal conditions.

ADVANCED SECURITY: Evidence is encrypted at rest on the camera to protect data at all times.

RAPIDLOCK MOUNTS: Versatile mounts keep the camera steady during tough situations.

MOBILE APP: Stream, tag, and replay videos right on your phone with Axon View.

APP AVAILABLE FOR
APPLE AND ANDROID

AXON BODY 2
SPECIFICATIONS

VIDEO RESOLUTION	Configurable up to 1080p
WEATHER RESISTANCE	IP67 (IEC 60529)
CORROSION RESISTANCE	MIL-STD-810G METHOD 509.5 (SALT FOG)
FIELD OF VIEW	142 degrees
OPERATING TEMPERATURE	-4 °F to 122 °F / -20 °C to 50 °C
DROP TEST	6 Feet
HUMIDITY	95% non-condensing
WARRANTY	1 year from date of receipt
RECORDING CAPACITY	Up to 70 hours depending on resolution

MPC0227 REV A

Axon Body 2 Camera Models

Model	Model No.	Color
Axon Body 2 camera	74001	Black

Specifications

1. Operating temperature range:
   −4 °F to 122 °F (−20 °C to 50 °C).
2. Storage temperature range:[1]
   −4 °F to 95 °F (−20 °C to 35 °C).
3. Charging temperature range:
   41 °F to 95 °F (5 °C to 35 °C).
4. Humidity: 95 percent non-condensing.
5. Drop test: 6-foot (1.8-meter).
6. IEC 60529 IP67 (6 dust, 7 water).
7. Salt fog MIL-STD-810G.
8. Up to 30 frames per second.
9. Settings: [2]

Resolution	File size for 1 h	Storage capacity
Low SD 480p (640 x 480 VGA resolution)	0.8 GB	>70 h
High SD 480p (640 x 480)	1.8 GB	~35 h
Low HD 720p (1280 x 720) (recommended)	2.7 GB	~23 h
High HD 1080p (1920 x 1080)	5.4 GB	~12 h

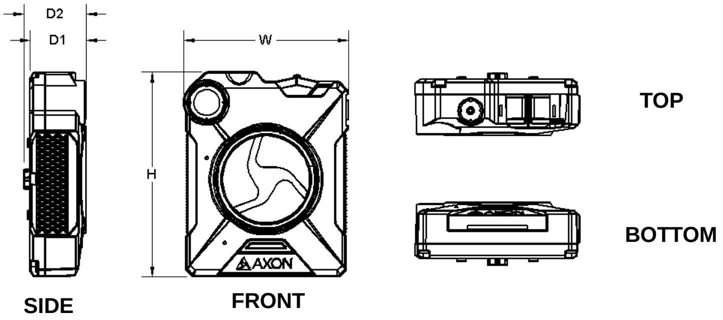
10. Specific absorption rate (SAR): 0.94 W/kg.
11. Rechargeable, replaceable lithium-ion polymer battery.
    3000 mAh capacity.[3,4]
12. Bluetooth 4.0.
13. USB 2.0.
14. Wi-Fi 802.11n at 5 GHz and 2.4 GHz.
15. More than 12 hours of battery life under normal operation.[5]
16. Video format: MPEG-4 (.MP4)
17. Video compression: H.264
18. Storage: 64 gigabyte solid-state non-removable embedded Multimedia Card (eMMC)
19. Encryption: 256-bit AES[2]
20. Light sensor: CMOS

Features

1. EVENT button to start and stop recording.
2. Pre-event buffer of 0–120 seconds, configurable by agency in 30-second increments.
3. On/Off slide switch to power the device.
4. Battery button and battery LED to indicate remaining battery capacity.
5. Operation LED on the top of the housing indicates camera status.
6. Dual-channel microphone: Stereo microphone (two-channel) always recording two tracks).
7. Haptic notification: Vibration feedback to accompany beep tones.
8. Near field communication (NFC) chip.
9. Several mounts are available.
10. Full color audiovisual camera.
11. 143° diagonal field of view camera lens. 107° horizontal field of view, and 78° vertical field of view.
12. Three-axis image stabilization.
13. Retina Low-Light capability less than 0.1 lux.
14. Playback and download via TASER software applications.
15. GPS tagging capability available through Android and iOS Axon View applications via Bluetooth technology. Streaming capability is available through Android and iOS Axon View applications via Wi-Fi technology.
16. Watermark: Date and time automatically embedded into the video.
17. Compatible with the Axon Signal Unit (ASU).

Physical Characteristics[6,7]

Dimensions				
Depth 1 (D1)	Depth 2 (D2)	Width (W)	Height (H)	Weight
0.94 in [2.4 cm]	1.01 in (2.6 cm)	2.76 in [7 cm]	3.42 in [8.7 cm]	5.0 oz [142 g]



[1] Less than 1 month at the high temperature. Long-term storage should be in a climate-controlled environment.
[2] Resolution and encryption settings are agency-configurable.
[3] Rechargeable lithium-ion polymer batteries have a limited life of approximately 1 year. With age, batteries will gradually lose their capacity to hold a charge. This loss of capacity (aging) is irreversible. As the battery loses capacity, the length of time it will power your device (run time) decreases. Additionally, lithium-ion polymer batteries continue to slowly discharge (self-discharge) when not in use or while in storage. It is advised that you routinely check the battery's charge status. The device should be recharged regularly to maintain the internal chemistry of the battery. TASER product user manuals summarize how to check battery status as well as battery charging instructions. The latest product manuals are available at www.taser.com.
[4] The Axon Body 2 camera battery pack can be replaced. Please contact www.taser.com to purchase a replacement battery.
[5] Temperature, other ambient conditions, and usage can affect battery life.
[6] Product specification may change without notice; actual product may vary from picture.
[7] Dimensions and weights are for reference only.

Axon Dock Models

Model	Model No.	Color
Axon Dock 6-Bay and Core[1]		Black

Specifications[2]

1. Input power requirements[3]
   Voltage: 15 V DC
   Current: 4 A DC
   Power: 60 W
   Connector: Barrel power connector, inner diameter 0.08″ [2.1 mm], outer diameter 0.22″ [5.5 mm], length 0.37″ [9.5 mm], inside positive
2. Output specifications per port
   Voltage: 4.5 V DC to 5.5 V DC
   Current: 1 A (maximum)
   Power: 2.75 W (maximum)
3. Operating Temperature: −4 °F [−20 °C] to 167 °F [75 °C]
4. Humidity: 85 percent non-condensing
5. One USB B input port, six 2.5 mm dock output ports, one USB A 2.0 output port

Features

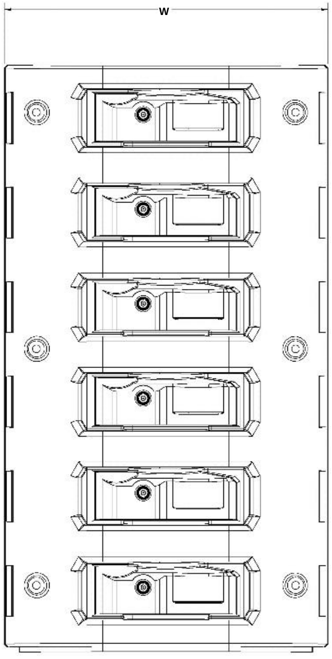
1. Modular design capable of managing six Axon Body 2 cameras.[4]
2. Status LED on the device docked in the bay indicates device status. Status can also be observed through web-based status screens.
3. Provides power to device docked in the bay to enable battery charging.

Characteristics

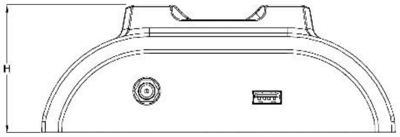
1. Attaches to Axon Dock core to connect to the Internet.

Physical Characteristics[2,5]

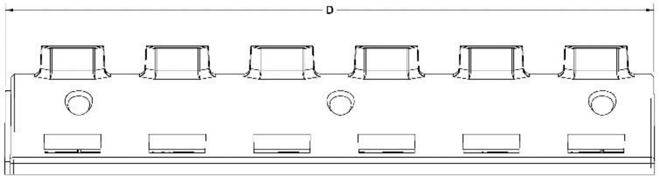
Width (W)	Height (H)	Depth (D)	Weight
6.4″ [16.2 cm]	2.18″ [5.5 cm]	11.25″ [28.6 cm]	1.36 lb. [612.35 g]



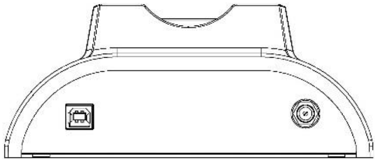
TOP VIEW



FRONT VIEW



SIDE VIEW



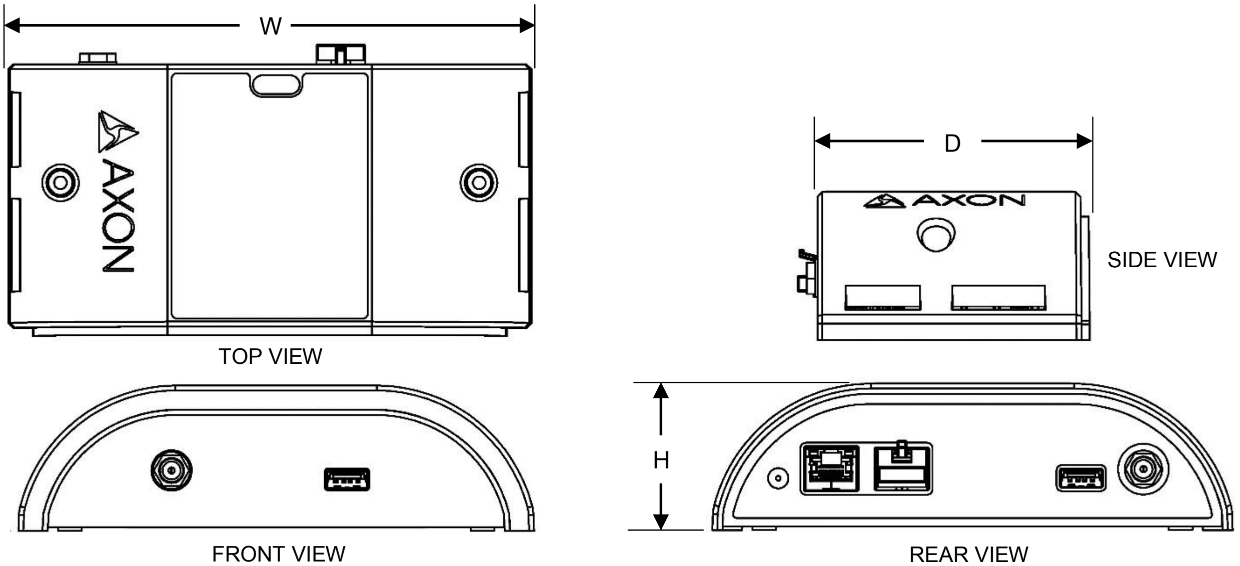
REAR VIEW

[1] This document only describes the bay. For information about the core, see the *TASER Axon Dock Core Specifications*.
[2] Product specification may change without notice; actual product may vary from picture.
[3] Required AC service specifications for provided external AC-DC power supply are 100–240 V AC, 1.5 A (min), 50–60 Hz.
[4] This 6-bay is designed for the Axon Body 2 camera. It will not work with Axon Body cameras or Axon Flex systems.
[5] Dimensions and weights are for reference only.

Axon Dock Core Models		
Model	**Model No.**	**Color**
Axon Dock Core Module	70027	Black

Specifications[1]	Features
1. Input power requirements[2] Voltage: 15 V DC Current: 4 A DC Connector: Barrel power connector, inner diameter 0.08″ [2.1 mm], outer diameter 0.22″ [5.5 mm], length 0.37″ [9.5 mm], inside positive 2. Output specifications per USB Port Voltage: 4.5 V DC to 5.5 V DC Current: 500 mA (maximum) Power: 2.75 W (maximum) 3. Operating Temperature: −4 °F [−20 °C] to 167 °F [75 °C] 4. Humidity: 85 percent non-condensing 5. Two CAT5E[3] Ethernet ports (one 100BASE-TX local area network (LAN[4]), one 1000BASE-T wide area network (WAN)) 6. Two USB A 2.0 ports **Characteristics** 1. Internet connection requirement: Ethernet 10BASE-T (LAN or WAN), 100BASE-TX (LAN or WAN), or 1000BASE-T (WAN)	1. Can be combined with all Axon Dock individual bay and 6-bay modules. 2. Provides secure connection to the Evidence.com[5] website from the device during transfer. 3. Device status can be observed through web-based status screens. 4. Provides power to device connected to the core to enable battery charging. 5. Diagnostic LEDs indicate power, LAN, WAN, and USB activity. 6. Dynamic and static IP capable network connection. 7. TASER web-based configuration interface. 8. Automatic firmware updates for TASER devices.

Physical Characteristics[1,6]			
Width (W)	Height (H)	Depth (D)	Weight
6.4″ [16.2 cm]	1.8″ [4.6 cm]	3.31″ [8.4 cm]	8.24 oz. [233.6 g]



[1] Product specification may change without notice; actual product may vary from picture.
[2] Required AC service specifications for provided external AC-DC power supply are 100–240 V AC, 1.5 A (min), 50–60 Hz.
[3] CAT5E cables must be used with the core.
[4] LAN is used for configuring the core. The LAN cannot be used to route network traffic.
[5] Subscription required.
[6] Dimensions and weights are for reference only.

GAIN A NEW PERSPECTIVE

THE LEADING POINT-OF-VIEW CAMERA, EVOLVED

Unmatched Durability | Best-in-Class Image Quality | Optimum Wearability

Gain a new perspective with the Axon Flex 2 camera. It brings point-of-view video to the next level, boasting a rugged industrial design, new mounts, and advanced capabilities like unlimited HD and a 120-degree field of view. Plus, it belongs to the growing Axon network of devices and apps that work together so you can focus on what matters - your job, not your technology.

800-978-2737 axon.io/flex2

AXON FLEX 2
FEATURES AND BENEFITS

BEST-IN-CLASS IMAGE QUALITY: The leading point-of-view camera now records in HD.

DUAL-CHANNEL AUDIO: Reduce ambient noise for improved sound quality.

WIDER FIELD OF VIEW: Capture more at the scene with a 120-degree field of view.

FULL-SHIFT BATTERY: Lasts for 12 hours of battery.

PRE-EVENT BUFFER: Capture up to 2 minutes before an event.

ENHANCED MOUNTS: Designed for versatility and optimum comfort.

UNMATCHED DURABILITY: Built to endure extreme field and weather conditions.

WIRELESS ACTIVATION: Axon Signal technology can sense certain events to activate your camera.

MOBILE COMPATIBILITY: Stream, tag, and replay footage right on your phone with the Axon View app.

EVIDENCE.COM INTEGRATION: Easily manage, retrieve, and share videos online.

APP AVAILABLE FOR
APPLE AND ANDROID

AXON FLEX 2
SPECIFICATIONS

WEATHER RESISTANCE IEC 60529 IP54 (dust, rain); MIL-STD-810G (Salt fog)

HOUSING High-impact polymer

FIELD OF VIEW 120 degrees

OPERATING TEMPERATURE -4 °F TO 122 °F [-20 °C TO 50 °C]

DROP TEST 6 feet

VIDEO MPEG-4 (MP4); H.264

HUMIDITY 95% non-condensing

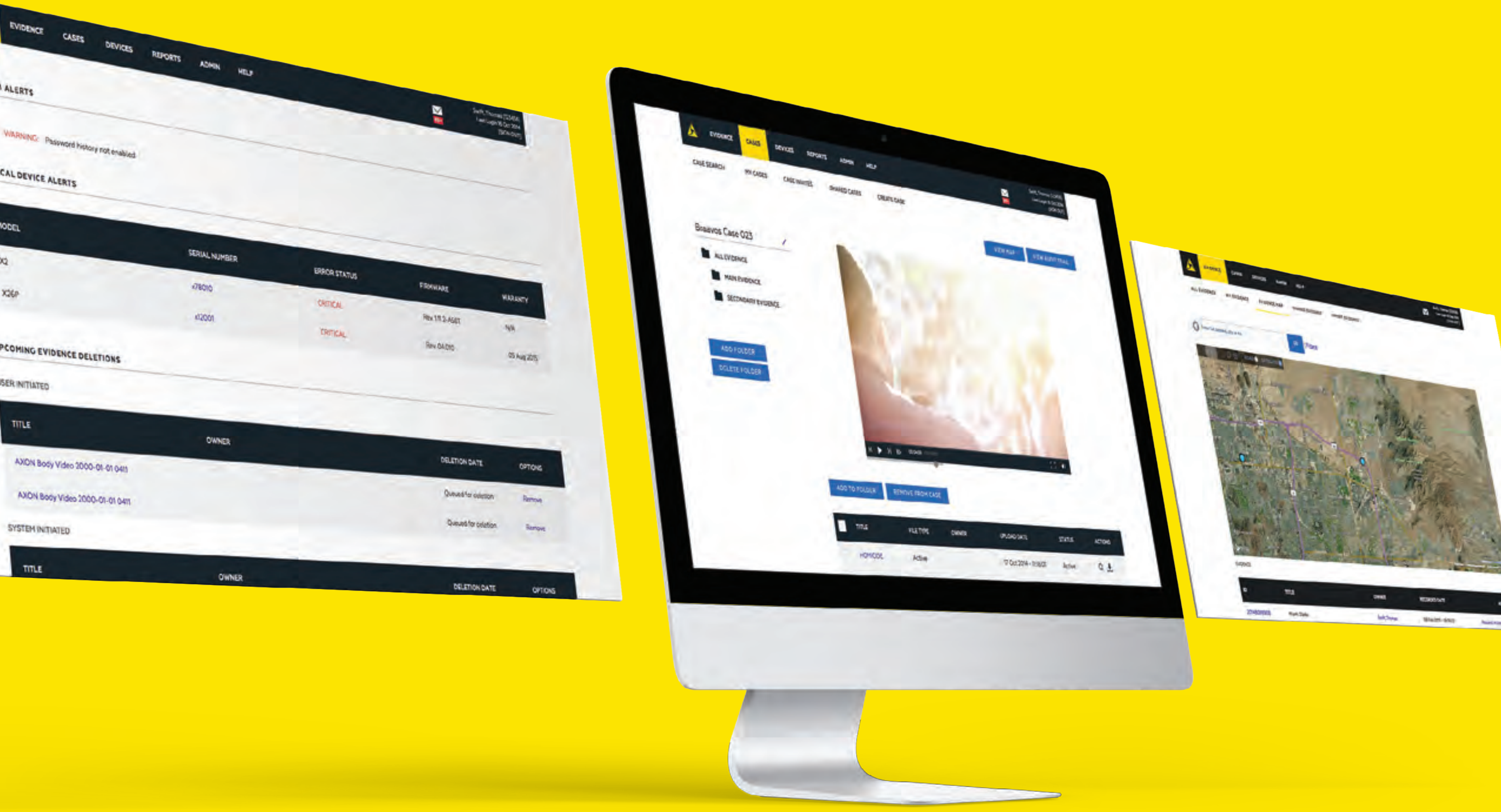
WARRANTY 1 year from date of receipt

RECORD TIME Up to 70 hours depending on resolution

ENCRYPTION 256-bit AES

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

AXON Evidence.com



MANAGE ALL OF YOUR DIGITAL EVIDENCE FROM CAPTURE TO COURTROOM

Evidence.com is a scalable, cloud-based system that consolidates all of your digital files, making them easy to manage, access and share while maintaining security and chain of custody.

UNIFY YOUR DIGITAL ASSETS

Eliminate data silos and manage all types of digital media from capture to courtroom, all with one secure system.

FASTER WORKFLOWS

Achieve the fastest speed of evidence processing through automation. Save time and money with industry-leading redaction technologies and secure digital sharing tools.

SCALABLE TECHNOLOGY

Enable deployments of any size with active directory integration, groups, reports, CAD/RMS Integration, automatic retention schedules and more.

THE AXON ADVANTAGE

Start immediately with no hardware to set up. Choose between plans with fixed or unlimited storage, and adjust instantly if needed. Stay up to date with free, automatic updates every month.

800-978-2737 axon.io/evidence

EVIDENCE.COM
FEATURES AND BENEFITS

LOWEST TOTAL COST OF OWNERSHIP: Evidence.com eliminates the cost of an in-house data center and the time associated with manual processes.

AVAILABILITY: Hosted securely in the cloud, Evidence.com can be accessed anytime, anywhere.

ONE-CLICK SEARCH: Search by officer name, incident ID, location and other tags to find files quickly.

CONFIGURABLE RETENTION: Schedule automatic retention periods based on incident type or crime severity.

CASE MANAGEMENT: Quickly view and share all digital files related by case number.

REDACTION SUITE: Save time with automated redaction, bulk redaction, clips, markers, thumbnails and more.

CAD/RMS INTEGRATION: Automate Axon video tagging by pulling in the correct metadata from existing systems.

PROSECUTOR WORKFLOW: Connect digitally with the prosecutor using the most scalable sharing solution available.

MOBILE INTEGRATION: Store and manage files captured with mobile devices in the field.

ANALYTICS AND AUDIT TOOLS: Monitor system usage, from total videos uploaded to who has reviewed, shared and deleted files.

EVIDENCE.COM
SECURITY FEATURES

CJIS-COMPLIANCE
Evidence.com is fully CJIS compliant.

AUDIT TRAIL AND CHAIN OF CUSTODY
Data is tamper-proof and all access events are reported in a secure audit trail.

CUSTOMIZABLE USER PERMISSIONS
Administrators can determine what files can be viewed by users and groups of users.

DATA ENCRYPTION
All information is fully encrypted in transit and at rest.

For more information, visit axon.io/security.

MPC0237 REV A

AXON

EVIDENCE.COM PLANS

Axon's Evidence.com services are available with pricing options that meet the needs of agencies of all sizes, starting at $15 per user per month. License levels allow you to choose from basic functionality to fully bundled plans that include hardware upgrades, warranties, and unlimited storage. See more at axon.io/pricing.

EVIDENCE.COM FEATURE TIERS			AXON CAMERA BUNDLES	
BASIC	**STANDARD**	**PRO**	**ULTIMATE**	**UNLIMITED**
Secure evidence storage Basic management tools Axon Capture Audit trails	All Basic features File and case sharing Bulk actions Admin roles	All Standard and Basic features Agency analytics Automated redaction Single sign-on / AD integration	All Pro features Axon camera upgrade every 2.5 yrs Extended Axon camera warranty Dedicated support & maintenance	All Ultimate features Unlimited HD storage* of Axon camera uploads Unlimited storage* of Axon Capture uploads
$15 user/month	$25 user/month	$39 user/month	$55 user/month	$79 user/month

AXON CAMERA + SMART WEAPON BUNDLE

OFFICER SAFETY PLAN:
Maximize officer safety and get the best value by bundling TASER Smart Weapons and body-worn cameras. The Officer Safety Plan offers complete budget predictability and keeps your technology up to date.

$99 user/month

*Unlimited data for Axon camera and Axon Capture uploads; additional storage is only 6.25¢ per GB per month.

AXON

AXON.IO/PRICING

EVIDENCE.COM PLANS	BASIC	STANDARD	PRO	ULTIMATE	UNLIMITED	OFFICER SAFETY PLAN
INCLUDED STORAGE	10GB	20GB	30GB	40GB	Unlimited Storage*	Unlimited Storage*
Axon Capture App	✓	✓	✓	✓	✓	✓
Evidence Sync	✓	✓	✓	✓	✓	✓
Dock-Automated Video Upload	✓	✓	✓	✓	✓	✓
Secure File Storage	✓	✓	✓	✓	✓	✓
Evidence Folders	✓	✓	✓	✓	✓	✓
GPS Mapping of Captured Media		✓	✓	✓	✓	✓
File & Case Sharing		✓	✓	✓	✓	✓
Video Clips & Markers		✓	✓	✓	✓	✓
Lock Specific Files for IA		✓	✓	✓	✓	✓
Custom User Roles		✓	✓	✓	✓	✓
Custom Categories		✓	✓	✓	✓	✓
Automatic File Deletion Schedules		✓	✓	✓	✓	✓
Bulk Reassign, Share, Edit		✓	✓	✓	✓	✓
User & Device Management		✓	✓	✓	✓	✓
Video Redaction			✓	✓	✓	✓
Operational Group Permissions			✓	✓	✓	✓
Agency Usage Reports			✓	✓	✓	✓
Active Directory Support			✓	✓	✓	✓
Two Axon Camera Upgrades†				✓	✓	✓
Full Axon Camera Warranty				✓	✓	✓
Unlimited HD Storage*					✓	✓
One Smart Weapon Upgrade†						✓
Full Smart Weapon Warranty						✓

†Applies to 5-year contracts only.
*Unlimited data for Axon camera and Axon Capture uploads; additional storage is only 6.25¢ per GB per month.

Other terms and conditions may apply and TASER reserves the right to change or end these offers at any time.

AXON

EVIDENCE.COM FOR PROSECUTORS

MANAGING EVIDENCE FROM CAPTURE TO COURT

As body camera footage and other forms of digital evidence become more prevalent, law enforcement agencies are faced with an unprecedented amount of data. That's why we offer Evidence.com for Prosecutors, a free evidence management solution that streamlines your workflow, making it manageable to handle agencies' growing amounts of evidence without having to grow your staff.

SHARE EVIDENCE WITH EASE

Evidence.com is easy to use. With a few clicks, you can add evidence to cases and share them with relevant parties, cutting a weeklong sharing process down to just minutes. Evidence.com also requires no ramp-up time to implement, and because of its instantly scalable, cloud-based system, increasing storage capacity is seamless.

KNOW YOUR DATA IS SECURE

We employ industry-leading security practices that have earned us the trust of thousands of agencies on our platform. Data is encrypted, and all actions are recorded in an audit log to ensure chain of custody and authenticity. That way, evidence managed through Evidence.com is still admissible in court.

DON'T BREAK YOUR BUDGET

We understand that attorneys don't always have the budgets that law enforcement agencies may have for new technology. Our standard plan lets you share cases, receive files from multiple agencies, upload digital data, instantly provide e-discovery, and more—for free. Plus, you won't have to hire additional staff to accommodate the influx of evidence. You can also redact footage, eliminating costs for external consultants.

STANDARD FEATURES

- Receive shared cases and share evidence externally for discovery
- Upload any type of digital data
- Add evidence to cases
- Create video clips and markers
- Customize user roles and permissions
- Set automated deletion schedules
- Bulk reassign, edit, and share

WANT TO LEARN MORE?

Contact us to hear about your options and to start your trial.

PROSECUTOR@EVIDENCE.COM 1-800-978-2737

EVIDENCE.COM PROSECUTOR LICENSES

PLAN	STANDARD	PRO
PRICE PER USER	FREE	$39/Month
STORAGE OF SHARED EVIDENCE	Unlimited	Unlimited
ADDITIONAL STORAGE PER MONTH	6.25¢/GB/Month	6.25¢/GB/Month
Receive Shared Cases	✓	✓
Share Evidence Externally for Discovery	✓	✓
Upload Any Type of Digital Data	✓	✓
Add Evidence to Cases	✓	✓
Create Video Clips and Markers	✓	✓
Customize User Roles and Permissions	✓	✓
Automated Deletion Schedules	✓	✓
Bulk Reassign, Share, Edit	✓	✓
Redact Videos		✓
Generate Agency Usage Reports		✓
Export Search Results to CSV		✓
Create Organizational Groups		✓
Single Sign-On		✓

AXON

MPC0219 REV F

TASER

Welcome to EVIDENCE SYNC.
Connect a device and select it from the Device list,

or select a Folder and choose photos, videos, and other evidentiary files to upload.

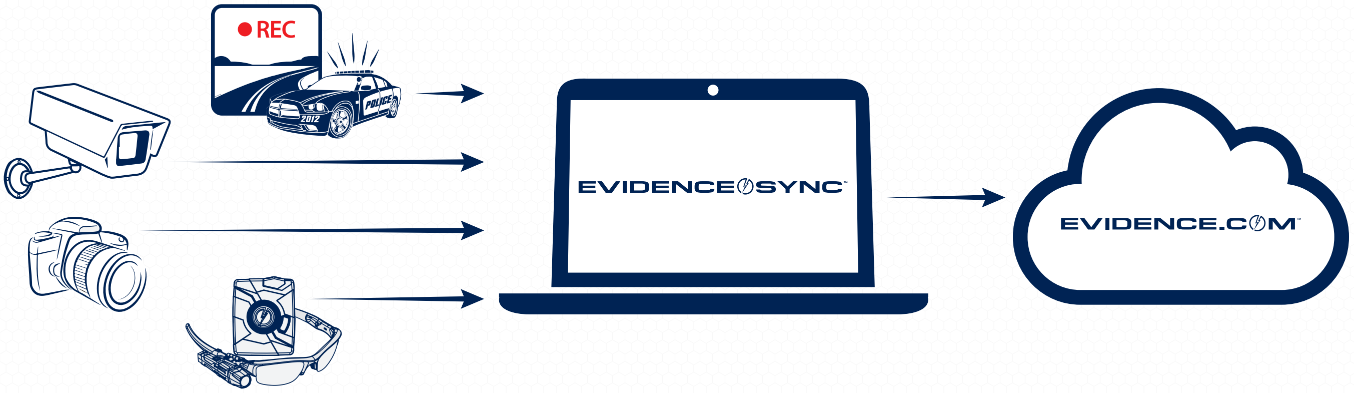
EVIDENCE Sync

- **Desktop Evidence Control** - Allows management of digital evidence and TASER® products from any computer with an internet connection, including an MDT.
- **Any File, Any Source** - Upload any audio, video, photo or other files currently on CDs, memory cards, servers or a hard drive to EVIDENCE.com.
- **Handsfree Transfer** - Select the data to upload to EVIDENCE.com, then log out and walk away while the app keeps working.

The newest version of EVIDENCE Sync makes your workflows easier and saves you time. Use Sync to preview, annotate and upload digital evidence from any source to EVIDENCE.com, plus manage your agency's TASER products and update firmware. And as always, your data is secure and easy to access at any point.

EVIDENCE.COM

▶ scan this QR code to learn more



FEATURES & BENEFITS

Upload Any Digital Evidence

Upload any format and size of photo, video or audio recording.

Manage TASER Products

Collect evidence, change settings, assign, and update firmware for your CEWs or AXON® cameras.

Add Metadata

Tag evidence with Title, Event ID, and Category, and assign evidence at upload.

Schedule Uploads

Select a folder or file on your hard drive or network to upload at set times.

Upload from Servers

Upload interview room or dash-cam videos from shared drives.

Upload from Camera, CD, or SD Card

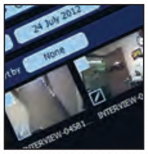
Upload crime scene photos from any source.

Upload from the Field

Run the app from your MDT and access from the field.

Walk Away During Uploads

Log out while uploads keep going in the background.



View Files in a Gallery

Quickly manage photos and videos using thumbnails.

Search Easily

Find any file and search by title, date, keyword or other fields.

MPC0195 REV A

EVIDENCE.COM

▸ scan this QR code to learn more

✉ Help@EVIDENCE.com ☎ 1.877.270.0553 Scottsdale, Arizona, U.S.A.

AXON Signal

NEVER MISS A CRITICAL INCIDENT

RECORD WITHOUT LIFTING A FINGER

Connect Devices | Improve Officer Safety | Eliminate Human Error

Critical event recording has become a major part of an officer's duties. With manual body camera activation, officers must remember to turn on their cameras at every incident. Oftentimes stress, adrenaline, and split-second time frames prevent this from happening consistently. Now, with Axon Signal, common triggers inside and outside of the squad car can automatically activate Axon cameras to capture vital footage that otherwise would be lost.

AXON SIGNAL FEATURES & BENEFITS

FLEXIBILITY: Axon Signal can be tailored to activate cameras based on various triggers such as light bar, crash, door and more.

CONNECTED PLATFORM: Integrates Axon cameras with TASER Smart Weapons and your vehicle.

30-FOOT RANGE: Activates all Axon cameras within a set radius to capture the most critical events.

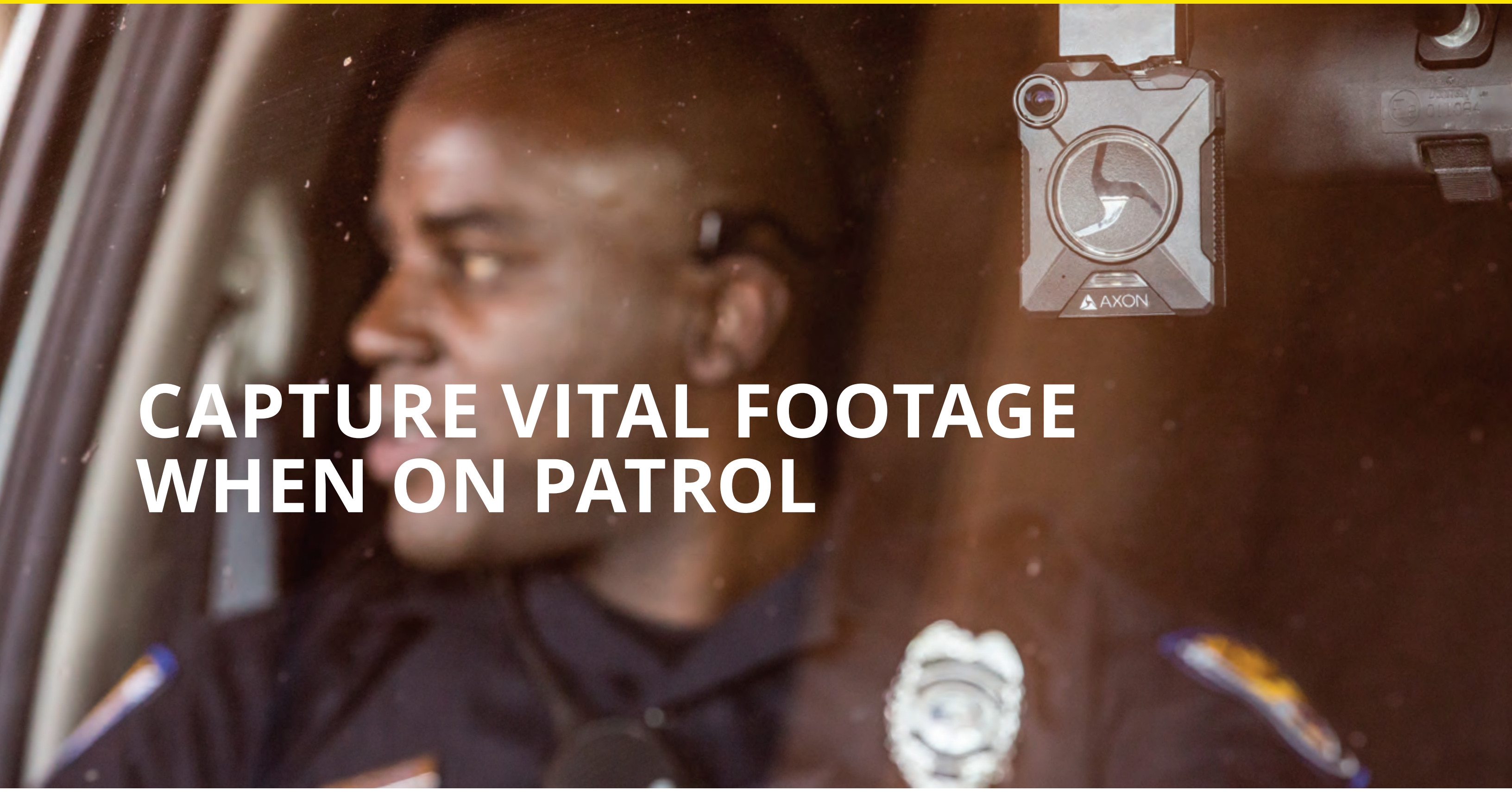
SECURE COMMUNICATION: A secure wireless connection protects your devices during use.

Axon Signal Vehicle Unit SKU: 70112

800-978-2737 axon.io/signal

CAM 17-0864
Exhibit 1

AXON Signal Unit



CAPTURE VITAL FOOTAGE WHEN ON PATROL

The Axon Signal Unit (ASU) activates Axon cameras in response to vehicle triggers, including when you turn on the light bar, open the door, or remove a weapon from the weapon rack. That way, you can focus on the critical situation in front of you - and not your camera.

FEATURES & BENEFITS

ACTIVATE CAMERAS: Activate your Axon Fleet, Axon Body 2, and Axon Flex cameras within 30 feet within 30 seconds.

MULTIPLE TRIGGERS: Select up to eight vehicle triggers to activate your cameras, like light bar, door, and weapon rack.

UNIVERSAL: Install the Axon Signal Unit in cars, SUVs, and motorcycles.

WHY SIGNAL UNIT?

IT'S EASY: Record events without lifting a finger. That way, you can focus on the situations in front of you.

IT TELLS A STORY: Collect key information about incidents, from the triggers that activate your camera to the video evidence you capture of a scene.

IT'S RELIABLE: Choose the triggers that will activate your camera, so your camera turns on when your department policy says it should.

Axon Signal Vehicle Unit SKU: 70112

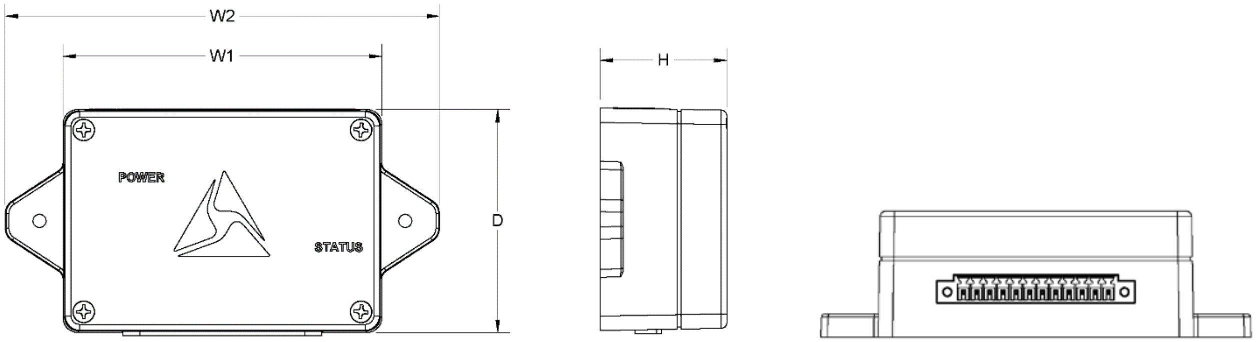
800-978-2737 axon.io/signal

REV A

Product Models[1]		
Model	**Model No.**	**Color**
Axon Signal Unit	70112	Black/Clear

Specifications	Features
1. Operating and storage temperature range: −40 °F to 176 °F [−40 °C to 80 °C] 2. Humidity: Up to 80% non-condensing 3. Bluetooth signal range: At least 30′ (9.14 m) (line of sight) 4. Operation Input Voltage: 5 V to 13.6 V 5. Ignition/Auxiliary Enable Voltage Threshold: 3.6 V 6. Maximum Current Draw: 25 mA Maximum while advertising Current Draw When Off: 40 µA Maximum 7. FCC and CE compliant 8. Vibration to ISO 16750-3 9. IEC 60529 IP5X dust protection	1. With emergency vehicle light bar activation, the Axon Signal Unit initiates the EVENT mode in an Axon system equipped with Axon Signal technology. 2. Power and Status LEDs to indicate unit functioning. 3. Connections include ignition enable, auxiliary enable, and 8 trigger inputs. 4. Advertisement Duration: 30 seconds per input Trigger Activation.

Physical Characteristics[2]				
Width 1 (W1)	Width 2 (W2)	Depth (D)	Height (H)	Weight
4.52″ (11.48 cm)	3.3″ (8.38 cm)	2.31″ (5.87 cm)	1.32″ (3.35 cm)	3.23 oz (91.58 g)



Top View

Side View

Back View

[1] Product specification may change without notice; actual product may vary from picture.

[2] Dimensions and weights are for reference only.

TASER

SIGNAL PERFORMANCE POWER MAGAZINE (SPPM)

Capture vital footage when you use your TASER Smart Weapon

The Signal Performance Power Magazine (SPPM) activates Axon cameras when your TASER X2 or X26P Smart Weapon is armed. That way, you can focus on the critical situation in front of you - and not your camera.

SPPM FEATURES & BENEFITS

INTEGRATE WEAPONS: Connect your TASER X2 or X26P Smart Weapon to the Axon platform.

ACTIVATE CAMERAS: Activate your Axon Fleet, Axon Body 2, and Axon Flex cameras within 30 feet within 30 seconds.

COLLECT INFORMATION: Log critical data points in your audit trail, like when your TASER Smart Weapon is armed, trigger is pulled, and arc is engaged.

WHY SPPM?

IT'S EASY: Record events without lifting a finger. That way, you can focus on the situations in front of you.

IT TELLS A STORY: Collect key information about incidents, from how you use your Smart Weapon to the video evidence you capture of a scene.

IT'S RELIABLE: Choose the triggers that will activate your camera, so your camera turns on when your department policy says it should.

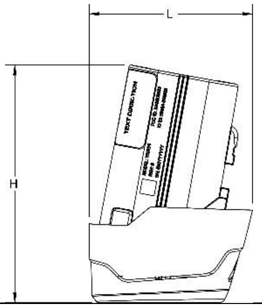
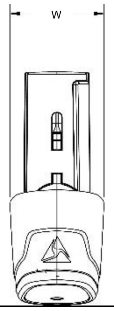
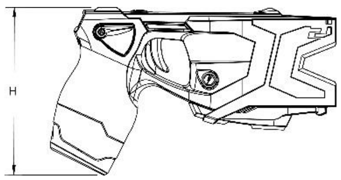
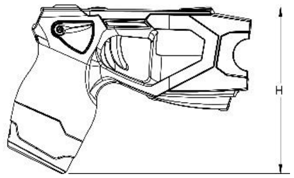
800-978-2737

X2 and X26P Conducted Electrical Weapon Signal Performance Power Magazine Models[1]

Model	Part No.	Color
Signal Performance Power Magazine (SPPM)	70116	Black

Specifications[2]	Features
1. Housing material: High impact polymer 2. Battery: Three lithium 3V cells 3. Operating and storage temperature range: –4 °F to 122 °F [–20 °C to 50 °C] 4. At room temperature 77 °F [25 °C], the SPPM provides energy for approximately 500 5-second discharges.[3,4,5,6] 5. Bluetooth Signal Range: Up to 100 feet (30.5 m)[7]	1. Designed for use with the X2 and X26P conducted electrical weapons (CEWs). 2. When the safety switch is shifted to the up (ARMED) position, the SPPM sends a signal to initiate the EVENT mode in an Axon system equipped with Axon Signal technology. 3. Secure Bluetooth transmission (30 seconds). 4. Moisture resistant when properly installed in the X2 and X26P CEWs.

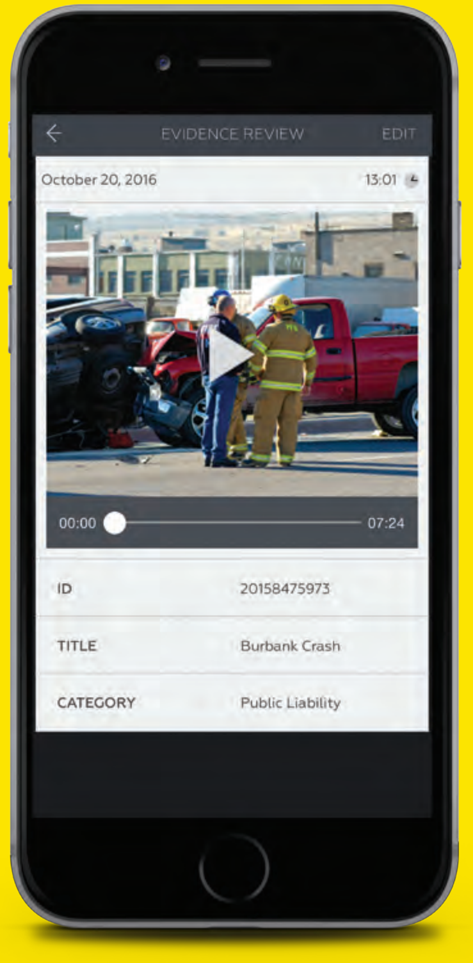
Physical Characteristics[2,8]

Characteristics				Dimensions (installed in TASER X2 CEW)	Dimension (installed in X26P CEW)
Length (L)	Height (H)	Width (W)	Weight	Height	Height
2.13″ [5.4 cm]	3.08″ [7.0 cm]	1.24″ [3.15 cm]	2.8 oz [79 g]	4.61″ [11.7 cm]	4.55″ [11.6 cm]
					

[1] Additional models available. Please contact a TASER International sales and customer service representative for more information.
[2] Product specifications may change without notice; actual product may vary from picture.
[3] The battery may lose 1 percent of its capacity per year. Estimated useful life: 5 years.
[4] Replace the SPPM when the battery percentage readout drops below 20 percent; continued use at 0% could cause damage to the CEW.
[5] Material Safety Data Sheets (MSDS) related to lithium cells are available upon request.
[6] Approximate firings figure is derived from controlled settings at room temperature; actual firings may be different due to environmental and usage variance.
[7] Range measurements are taken line-of-sight with nothing blocking transmission paths. Actual results may vary depending on environmental obstructions.
[8] Dimensions and weights are for reference only.

AXON View

INSTANT VIDEO PLAYBACK IN THE FIELD



October 20, 2016 13:01

00:00 07:24

ID	20158475973
TITLE	Burbank Crash
CATEGORY	Public Liability

AXON VIEW

See what your camera sees

TURN ROUTINE VIDEO INTO VALUABLE EVIDENCE

Live Feed | GPS Tagging | Metadata Input

Axon View is a mobile application that wirelessly connects with your Axon camera to provide instant playback of unfolding events in the field. Axon View automatically maps video with GPS data and allows real-time tagging of metadata, such as Case ID and Category, from your phone. Before you set foot in the station, your video is automatically filed into the correct case report and retention schedule.

800-978-2737 axon.io/view

AXON VIEW
FEATURES & BENEFITS

INSTANT REPLAY: Prevent frivolous disputes over recorded events

MOBILE TAGGING: Input data on the scene for easy searching and accurate retention

GPS: Map video evidence automatically

LIVE STREAMING: Achieve optimal camera placement

SECURE STORAGE: Information is viewed but not stored on the mobile device

APP AVAILABLE FOR
APPLE AND ANDROID

AXON VIEW
SPECIFICATIONS

IOS:

Requires iOS 6.1 or later. Compatible with iPhone, iPad, and iPod touch.
This application is optimized for iPhone 5.
Size: 5.9 MB
Language: English

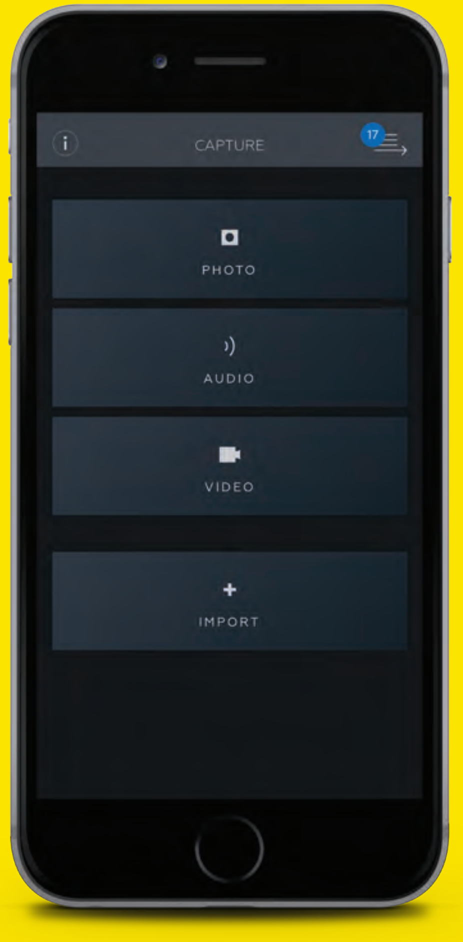
ANDROID:

Requires Android 2.3.3 and up
Size: 6.4 MB
Language: English

Android is a trademark of Google, Inc., IOS is a trademark of Cisco Technology, Inc., and Apple, the Apple logo, iPhone, iPad and iPod touch are trademarks of Apple, Inc. The Android robot is reproduced or modified from work created and shared by Google and used according to terms described in the Creative Commons 3.0 Attribution License.

AXON Capture

COLLECT EVIDENCE AND UPLOAD FROM THE FIELD



No more wires and SD cards

CARRY LESS. CAPTURE MORE.

Digital Photos | Audio Recordings | Cell Phone Videos

Axon Capture is a mobile application built specifically for law enforcement that allows officers to capture digital evidence right from the field. The application eliminates the need to carry multiple devices for photo, video and audio recording. Instead, it uses the capabilities of the smartphone already in your pocket and adds the security and organization needed to protect truth. You can add tags, titles or GPS coordinates to any recording before uploading the data to Evidence.com, without leaving anything on your phone.

800-978-2737 axon.io/capture

AXON CAPTURE FEATURES & BENEFITS

SIMPLIFIED WORKFLOW: Leverages smartphone features for data capture

GPS: Automatically tags photos and videos with location data

CONNECTED PLATFORM: Integration with Evidence.com is seamless

MOBILE TAGGING: Directly add metadata from the scene

APP AVAILABLE FOR
APPLE AND ANDROID

AXON CAPTURE SPECIFICATIONS

COMPATIBILITY

Android: Compatible with Android Devices Version 2.3 and above
iOS: Compatible with Apple iOS 6.0 and above on iPhone, iPad, and iPod touch

UPLOAD METHOD

Upload data via any 3G or 4G data connection, or via a Wifi connection

ACCESS

Users must log in to their active Evidence.com account to use the application

STORAGE

The application will only upload data to Evidence.com secured storage

LANGUAGE

Available in English and Spanish

AXON

EVIDENCE.COM AND AXON CAPTURE

REDMOND PD CASE STUDY

OVERVIEW

Before implementing Evidence.com and Axon Capture, a mobile evidence collection app, Redmond PD was spending a significant amount of time and money uploading and storing their digital evidence using an on-premise system. According to Redmond PD Commander Erik Scairpon, "It currently takes 30 minutes out of an officer's day to upload digital evidence to their current system, and that is a conservative estimate." With Evidence.com and Axon Capture, officers can capture, add metadata to, and upload images from the field. After Redmond's trial run, they estimate they will save over $1,100 per officer a year with this program.

USER FEEDBACK

After the trial, when asked how successful officers thought Evidence.com would be as their primary form of digital evidence storage, they responded with resoundingly positive feedback. Officers reported Evidence.com combined with Axon Capture was "really successful," "easy for pictures," and "compared to what we have, more efficient." Axon Capture's ability to allow officers to upload images from a scene using their smartphones was considered extremely helpful, especially because it allowed crime analysts to start looking at images faster than ever before.

STATS

- **39** total participants (23 with high/moderate use of system)
- **$1,145** estimated annual savings per officer
- **306.5%** ROI

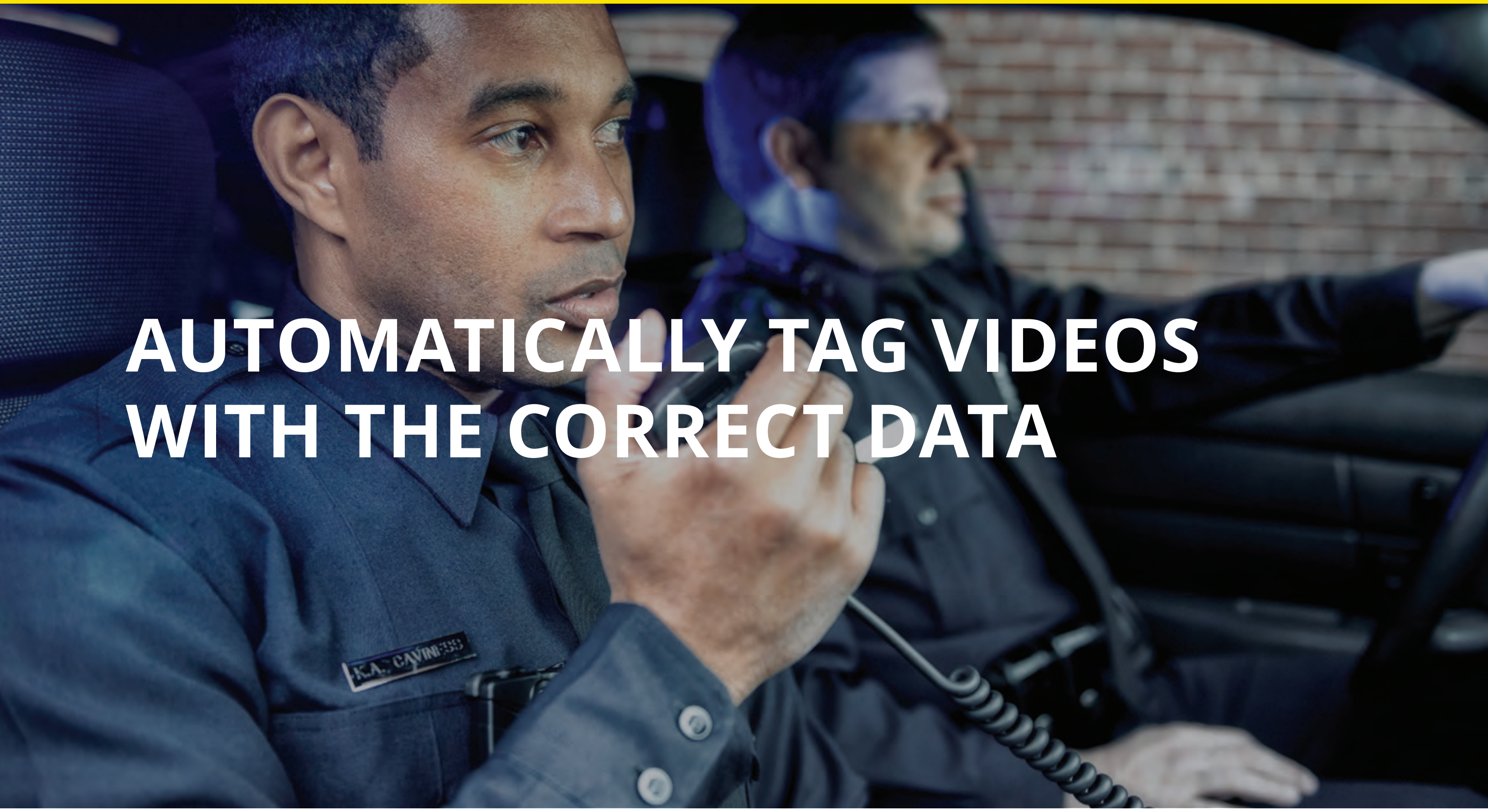
ABOUT REDMOND PD, WASHINGTON

- **85** commissioned officers
- **17** square miles
- **56-57,000:** Approximate civilian population

axon.io/evidence

AXON

CAD/RMS INTEGRATION



AUTOMATICALLY TAG VIDEOS WITH THE CORRECT DATA

CAD/RMS Integration takes information from your Computer-Aided Dispatch and Records Management System and ties it to your videos on Evidence.com. Agencies use it to:

IMPROVE ACCURACY

- Adds Incident ID, Category, Location and other tags to videos automatically
- Avoids the misspellings and incomplete information of manual entry
- Makes it easier to search and retrieve Axon videos later

SAVE TIME

- Frees officers from manual video tagging
- Requires minimal involvement from agency IT staff
- No need to involve CAD or RMS providers

REDUCE COST

- Saves up to $200 per officer per month in productivity costs
- Per-user pricing scales with the number of officers uploading
- Can be added to existing Evidence.com contracts anytime

800-978-2737 axon.io/cad-rms

FAQs ABOUT CAD/RMS INTEGRATION

Q: WHAT IS EVIDENCE.COM CAD/RMS INTEGRATION?
A: We take information exported from the agency's Computer Aided Dispatch and/or Records Management System and correlate it with videos on Evidence.com, allowing us to automatically tag Axon videos with the correct Incident ID, Category, Location and other information.

Q: WHY IS CAD/RMS INTEGRATION VALUABLE?
A: Video evidence can be invaluable—as long as it's easily logged and found. We've observed that when busy officers manually tag videos with metadata, many videos are tagged with the incorrect information or aren't even tagged. CAD/RMS Integration automates the process, taking human error out of the equation to ensure that you have complete, correct information.

Q: HOW MUCH TIME DOES IT TAKE TO MANUALLY TAG VIDEOS?
A: Manually tagging a video takes up to 3 minutes of an officer's time. If officers record 5 videos per shift and work 16 shifts per month, that means each officer spends 4 hours per month entering metadata. Some agencies estimate that an automated process could help reduce productivity costs by $200 each month for every officer. That's on top of the efficiency gains from implementing Axon cameras and Evidence.com in the first place.

Q: HOW DOES IT WORK?
A: We can integrate with any CAD or RMS system, without involving your system's vendor in the process.

For your agency there are only 2 steps:

1. Generate a regularly scheduled export (CSV file) of your CAD or RMS database with the relevant information.

2. Install a secure application behind your firewall to encrypt the exported file and send it to Evidence.com, where customized software automatically ties the correct metadata to the appropriate videos.

When officers next log in, their videos will all be automatically tagged with the correct data. When supervisors search for videos, they can be confident that their results are comprehensive. Generally a CAD/RMS Integration takes only 4–8 weeks to implement, although this depends on coordination with the agency's IT department.

Q: HOW MUCH DOES IT COST?
A: CAD/RMS Integration uses a license model, which includes a per-user monthly fee. The total cost for an agency will vary based on the number of users uploading Axon videos. Your TASER Sales Representative can provide you with an accurate quote and notify you of any current promotions. You can add CAD/RMS Integration to your current Evidence.com contract at any time.

Q: HOW DO I GET STARTED OR LEARN MORE?
A: If you are interested in an Evidence.com CAD/RMS Integration for your agency, or just want to learn more, please contact your TASER Sales Representative or visit **axon.io/cad-rms**.

AXON

AUTOMATING MANUAL TAGGING

CAD/RMS INTEGRATION CASE STUDY

OVERVIEW

Before deploying CAD/RMS Integration, officers in Peoria, Arizona were spending significant time manually tagging videos, a process that often resulted in incorrect or missing information. On average, agencies find that the error rate for manual tagging is 33%, making it difficult for supervisors to find videos when they're needed later. Axon's CAD/RMS Integration automatically tags Axon videos with the correct information found in CAD calls and RMS cases such as Officer Name, Incident ID and Location. Not including back-end administrative time savings, Peoria is saving $2,500 per officer per year in freed time.

THE INTEGRATION PROCESS

No CAD or RMS vendor involvement is necessary. Instead, TASER sales engineers work with agency IT staff to integrate CAD and RMS systems with Evidence.com. Once completed, the integration requires minimal maintenance.

> *"In December 2014, the City of Peoria implemented TASER body-worn camera devices. TASER was exceptional in partnering with our agency as they created a solution that allows our officers to utilize the body-worn camera and not have to manage numerous hours of administrative tasks on the back end. Upon its completion, we have found this data integration will save us thousands of dollars in data entry hours."*
>
> - **City of Peoria Police Chief Roy W. Minter, Jr.**

STATS

- **54** RMS Integration Licenses
- **$135,000** Total Annual Savings
- **1390%** ROI
- **99.94%** Tagging Accuracy

ABOUT PEORIA PD, ARIZONA

- Sworn: **193**
- Axon Cameras Deployed: **54**
- Civilian Population: **164,825**

axon.io/cad-rms

AXON

AXON PROFESSIONAL SERVICES:

	STARTER PACKAGE $2,500	FULL-SERVICE PACKAGE $15,000
COVERAGE	No unit limit	No unit limit
SESSION DURATION	1 Day	Up to 4 Days
ADMIN TRAINING / DELIVERY		
Evidence.com Configuration	Virtual	On-site
Axon Dock Configuration	Virtual	On-site
Axon Device Configuration	Virtual	On-site
System Admin, Armorer, Records Training	On-site	On-site
USER TRAINING & ACCOUNT MANAGEMENT		
End User Go-Live Training	On-site* (One session)	On-site (Two days, up to six sessions)*
On-site Train-the-Trainer	—	Yes
Dedicated Project Manager	—	Yes
Weekly Project Planning Call	—	Yes
Customized Project Plan	—	Yes

*Additional training days offered at $2,000 per day.

Evidence.com features a full redaction suite natively within the application. This functionality is available to all licensed users, subject to your agency's role-based access controls.

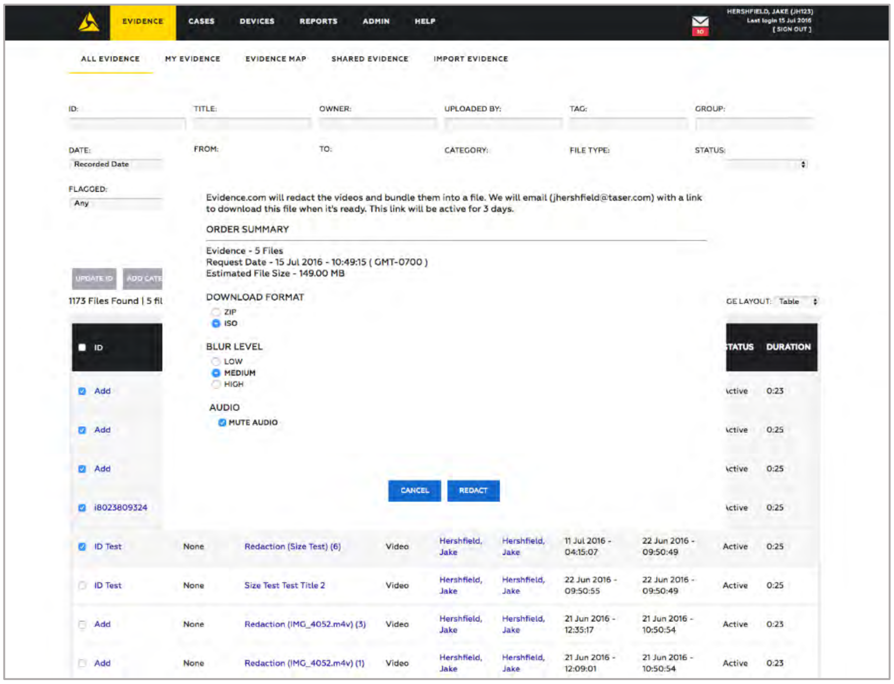
Evidence.com offers both automated and manual options for redacting an evidence file (or multiple evidence files). A full description of the comprehensive redaction capabilities within Evidence.com follows.

EVIDENCE.COM REDACTION SUITE OVERVIEW

Evidence.com offers users three options to redact videos, each to be used in a different scenario: **Bulk Redaction, Smart Tracker Redaction and Manual Redaction**. Both Bulk and Smart Tracker Redaction options are automated. Each of these options are simple and easy to use, allowing the FLPD personnel to manage public information requests quickly.

Bulk Redaction

To aid with large public disclosure requests, the Bulk Redaction feature allows a user to queue video evidence for bulk redaction. Bulk redaction creates a copy of the original video and a blur filter over the *entire* video automatically. It can also remove audio for the duration of that copy. 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.



ID:
TITLE:
OWNER:
UPLOADED BY:
TAG:
GROUP:
DATE: Recorded Date
FROM:
TO:
CATEGORY:
FILE TYPE:
STATUS:
FLAGGED: Any

Evidence.com will redact the videos and bundle them into a file. We will email (jhershfield@taser.com) with a link to download this file when it's ready. This link will be active for 3 days.

ORDER SUMMARY

Evidence - 5 Files
Request Date - 15 Jul 2016 - 10:49:15 (GMT-0700)
Estimated File Size - 149.00 MB

DOWNLOAD FORMAT
○ ZIP
● ISO

BLUR LEVEL
○ LOW
● MEDIUM
○ HIGH

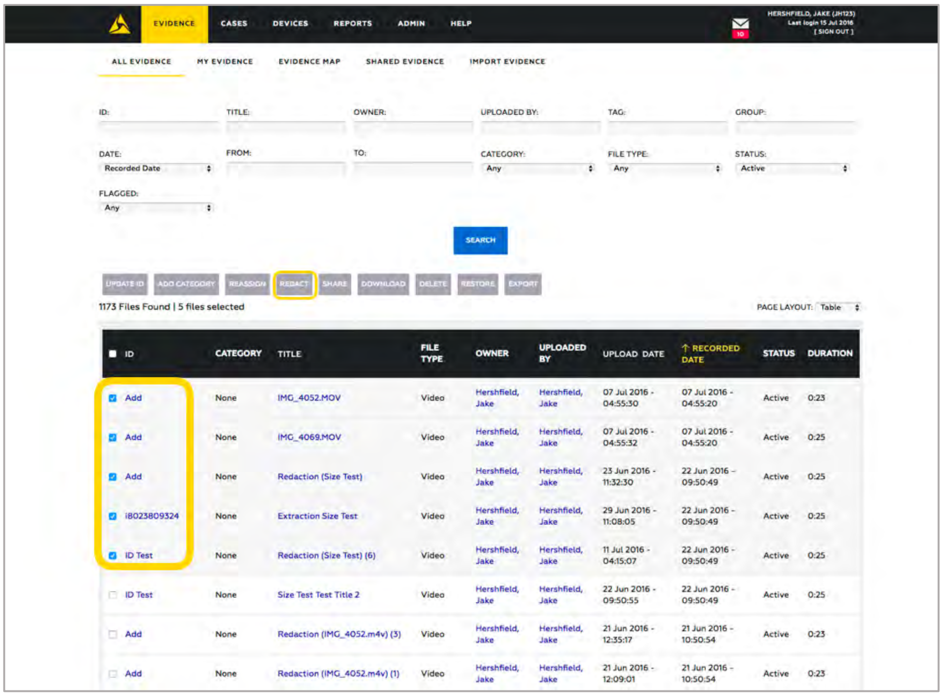
AUDIO
☑ MUTE AUDIO

1173 Files Found | 5 fil

GE LAYOUT: Table

□ ID								TATUS	DURATION
☑ Add								\ctive	0:23
☑ Add								\ctive	0:25
☑ Add								\ctive	0:25
☑ i8023809324								\ctive	0:25
☑ ID Test	None	Redaction (Size Test) (6)	Video	Hershfield, Jake	Hershfield, Jake	11 Jul 2016 - 04:15:07	22 Jun 2016 - 09:50:49	Active	0:25
□ ID Test	None	Size Test Test Title 2	Video	Hershfield, Jake	Hershfield, Jake	22 Jun 2016 - 09:50:55	22 Jun 2016 - 09:50:49	Active	0:25
□ Add	None	Redaction (IMG_4052.m4v) (3)	Video	Hershfield, Jake	Hershfield, Jake	21 Jun 2016 - 12:35:17	21 Jun 2016 - 10:50:54	Active	0:23
□ Add	None	Redaction (IMG_4052.m4v) (1)	Video	Hershfield, Jake	Hershfield, Jake	21 Jun 2016 - 12:09:01	21 Jun 2016 - 10:50:54	Active	0:23

It is recommended that a user verifies bulk-redacted videos to ensure the proper level of blur is applied to each file prior to releasing the redacted version. If a user needs to redact a video more precisely, such as redacting only a portion of each video frame, they can redact a single video.



ID:
TITLE:
OWNER:
UPLOADED BY:
TAG:
GROUP:
DATE: Recorded Date
FROM:
TO:
CATEGORY: Any
FILE TYPE: Any
STATUS: Active
FLAGGED: Any

1173 Files Found | 5 files selected

PAGE LAYOUT: Table

□ ID	CATEGORY	TITLE	FILE TYPE	OWNER	UPLOADED BY	UPLOAD DATE	↑ RECORDED DATE	STATUS	DURATION
☑ Add	None	IMG_4052.MOV	Video	Hershfield, Jake	Hershfield, Jake	07 Jul 2016 - 04:55:30	07 Jul 2016 - 04:55:20	Active	0:23
☑ Add	None	IMG_4069.MOV	Video	Hershfield, Jake	Hershfield, Jake	07 Jul 2016 - 04:55:32	07 Jul 2016 - 04:55:20	Active	0:25
☑ Add	None	Redaction (Size Test)	Video	Hershfield, Jake	Hershfield, Jake	23 Jun 2016 - 11:32:30	22 Jun 2016 - 09:50:49	Active	0:25
☑ i8023809324	None	Extraction Size Test	Video	Hershfield, Jake	Hershfield, Jake	29 Jun 2016 - 11:08:05	22 Jun 2016 - 09:50:49	Active	0:25
☑ ID Test	None	Redaction (Size Test) (6)	Video	Hershfield, Jake	Hershfield, Jake	11 Jul 2016 - 04:15:07	22 Jun 2016 - 09:50:49	Active	0:25
□ ID Test	None	Size Test Test Title 2	Video	Hershfield, Jake	Hershfield, Jake	22 Jun 2016 - 09:50:55	22 Jun 2016 - 09:50:49	Active	0:25
□ Add	None	Redaction (IMG_4052.m4v) (3)	Video	Hershfield, Jake	Hershfield, Jake	21 Jun 2016 - 12:35:17	21 Jun 2016 - 10:50:54	Active	0:23
□ Add	None	Redaction (IMG_4052.m4v) (1)	Video	Hershfield, Jake	Hershfield, Jake	21 Jun 2016 - 12:09:01	21 Jun 2016 - 10:50:54	Active	0:23

Smart Tracker Redaction

Smart Tracker Technology within Evidence.com brings intelligent, automated support to agency video redaction workload. Using the Smart Tracker technology, users can easily create a redaction that tracks up to 10 objects in a video. For each object, specify a start and end frame. On each start frame, place and size a redaction mask.

Once a user is done preparing assisted redaction, Evidence.com's technology tracks the redacted objects automatically and sends a notification email when it has finished creating the redaction.

It is recommended that users closely verify redacted clips created using assisted redaction. If corrections are necessary, Evidence.com allows for manual edits to redacted clips.

Smart Tracker Technology Concepts

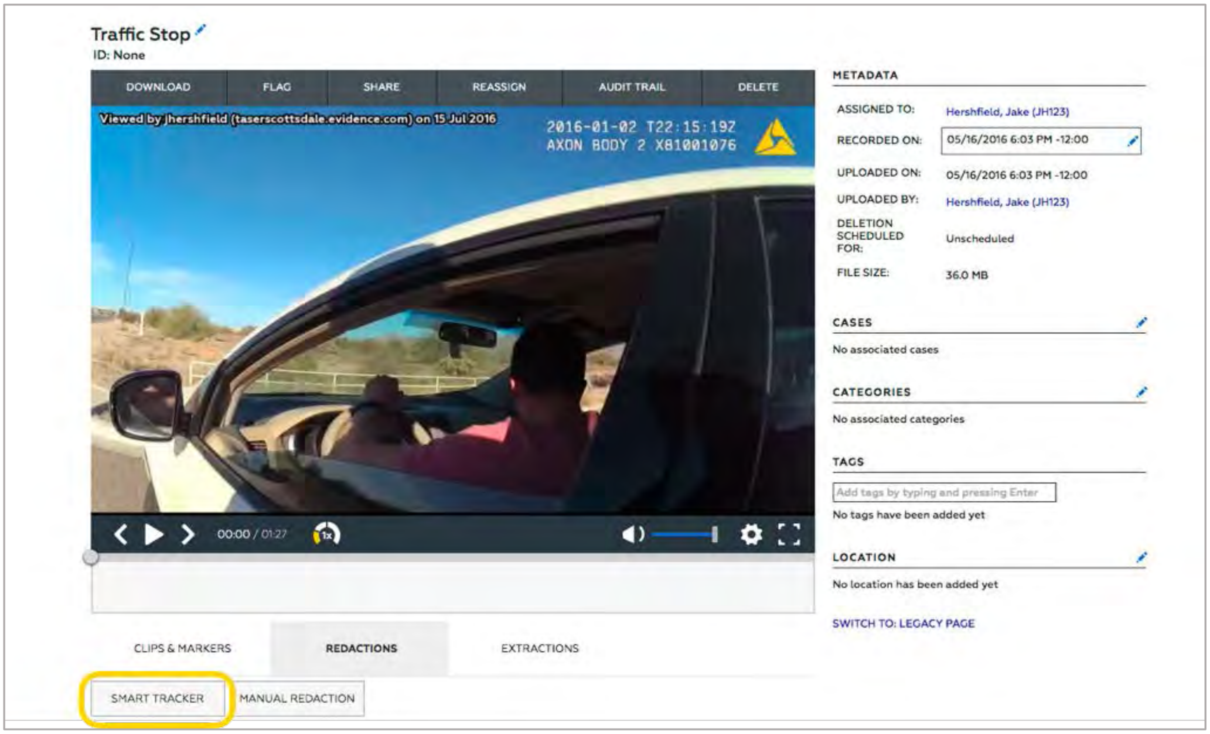
Using Smart Tracker technology to create a redaction shares many concepts with manual redaction. Because Smart Tracker technology automatically tracks objects in the video file, the Smart Tracker feature represents an object and its timeline with one control, eliminating the need to create multiple mask timelines per object.

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

- **Object Timeline**—Represents all frames in the video and enables users to place the mask segment precisely where it is needed. Each Smart Tracker object timeline has one mask segment.

Smart Tracker Technology Controls

On each start frame, position the redaction mask and when preparation of assisted redaction is complete, Evidence.com tracks the redacted objects automatically and notifies the user when tracking is complete. A user can then verify the redaction as closely as needed. If corrections are needed, Evidence.com allows manual adjustments.



Traffic Stop

ID: None

METADATA

ASSIGNED TO:	Hershfield, Jake (JH123)
RECORDED ON:	05/16/2016 6:03 PM -12:00
UPLOADED ON:	05/16/2016 6:03 PM -12:00
UPLOADED BY:	Hershfield, Jake (JH123)
DELETION SCHEDULED FOR:	Unscheduled
FILE SIZE:	36.0 MB

CASES

No associated cases

CATEGORIES

No associated categories

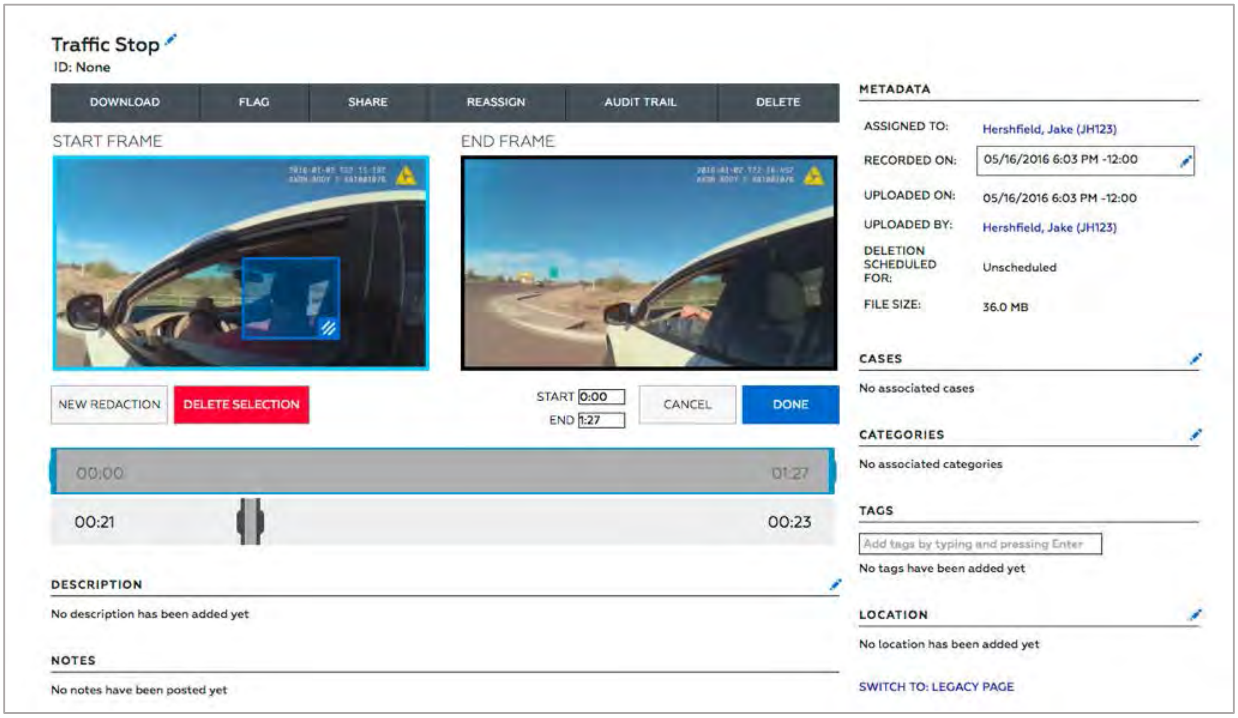
TAGS

Add tags by typing and pressing Enter

No tags have been added yet

LOCATION

No location has been added yet



Traffic Stop

ID: None

START 0:00

END 1:27

METADATA

ASSIGNED TO:	Hershfield, Jake (JH123)
RECORDED ON:	05/16/2016 6:03 PM -12:00
UPLOADED ON:	05/16/2016 6:03 PM -12:00
UPLOADED BY:	Hershfield, Jake (JH123)
DELETION SCHEDULED FOR:	Unscheduled
FILE SIZE:	36.0 MB

CASES

No associated cases

CATEGORIES

No associated categories

TAGS

Add tags by typing and pressing Enter

No tags have been added yet

LOCATION

No location has been added yet

DESCRIPTION

No description has been added yet

NOTES

No notes have been posted yet

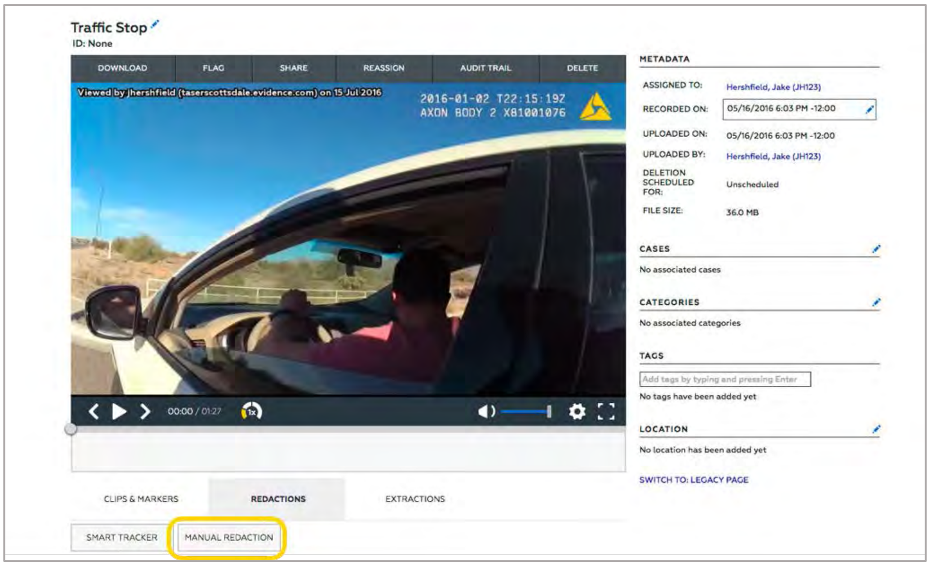
Manual Redaction

Manual redaction allows the user to control size, shape, and placement of redaction masks precisely, frame by frame.

Manual Redaction Concepts

Creating a redaction manually involves working with several important concepts.

- **Object**—Organizes the mask segments that redact one actual object in the video. A redaction contains one or more objects. An object contains one or more mask timelines.
- **Mask**—Defines a rectangular area in a continuous segment of video frames that are redacted. A mask has 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.
- **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.
- **Mask Frame Handle**—Enables you to change the size and shape of the mask frame.



Traffic Stop
ID: None

Viewed by jhershfield (taserscottsdale.evidence.com) on 15 Jul 2016
2016-01-02 T22:15:19Z
AXON BODY 2 X81001076

00:00 / 01:27

METADATA

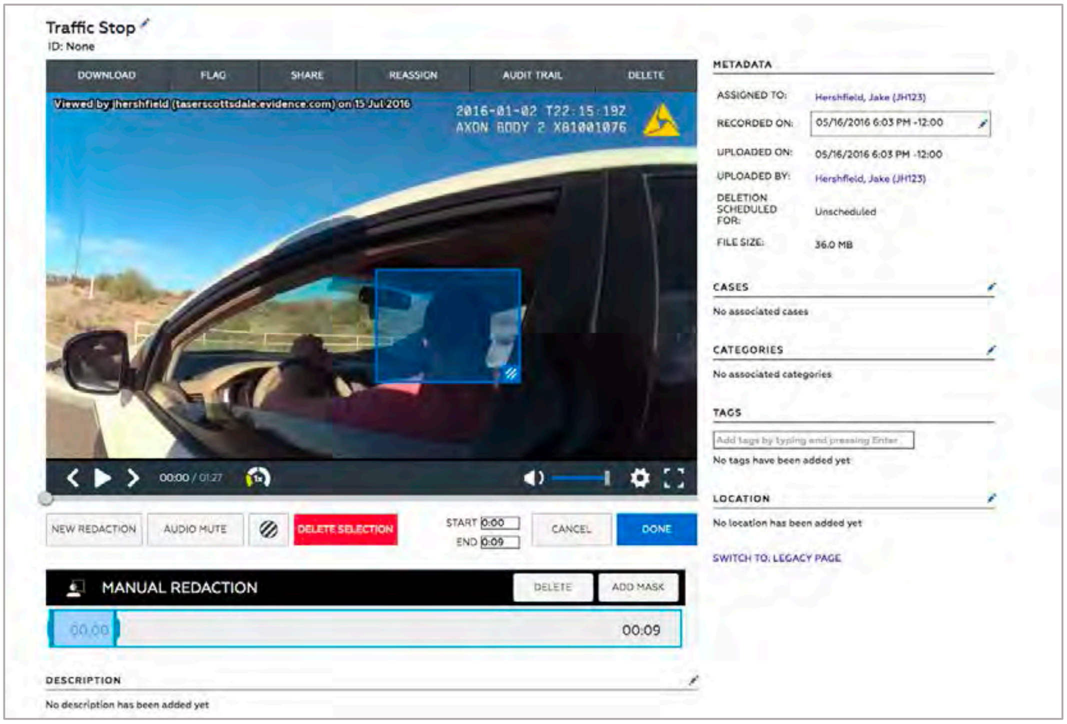
ASSIGNED TO: Hershfield, Jake (JH123)
RECORDED ON: 05/16/2016 6:03 PM -12:00
UPLOADED ON: 05/16/2016 6:03 PM -12:00
UPLOADED BY: Hershfield, Jake (JH123)
DELETION SCHEDULED FOR: Unscheduled
FILE SIZE: 36.0 MB

CASES
No associated cases

CATEGORIES
No associated categories

TAGS
Add tags by typing and pressing Enter
No tags have been added yet

LOCATION
No location has been added yet



Traffic Stop

ID: None

START 0:00

END 0:09

DESCRIPTION

No description has been added yet

METADATA

ASSIGNED TO: Hershfield, Jake (JH123)

RECORDED ON: 05/16/2016 6:03 PM -12:00

UPLOADED ON: 05/16/2016 6:03 PM -12:00

UPLOADED BY: Hershfield, Jake (JH123)

DELETION SCHEDULED FOR: Unscheduled

FILE SIZE: 36.0 MB

CASES

No associated cases

CATEGORIES

No associated categories

TAGS

Add tags by typing and pressing Enter

No tags have been added yet

LOCATION

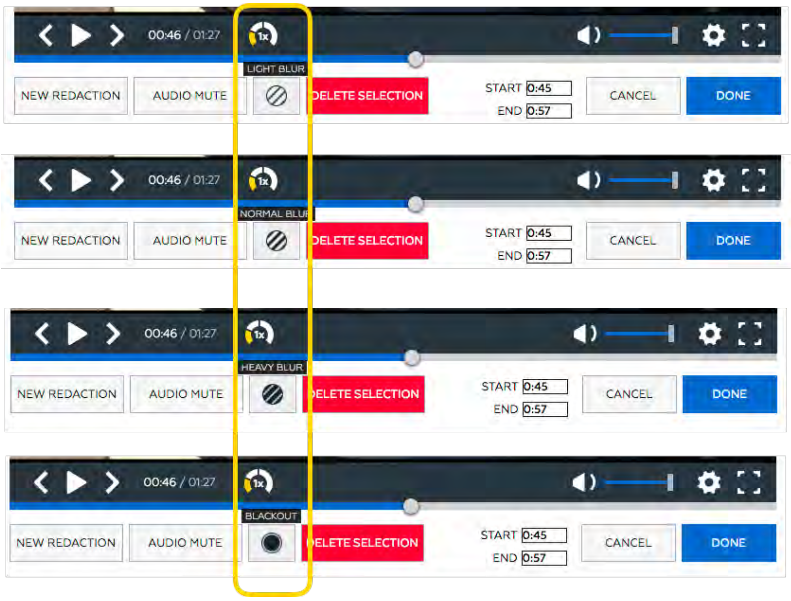
No location has been added yet

SWITCH TO: LEGACY PAGE

Additional Functionality

Blur Levels

Users can toggle the blur level of the redaction masks from low, medium, high, and blackout blur.



START 0:45

END 0:57

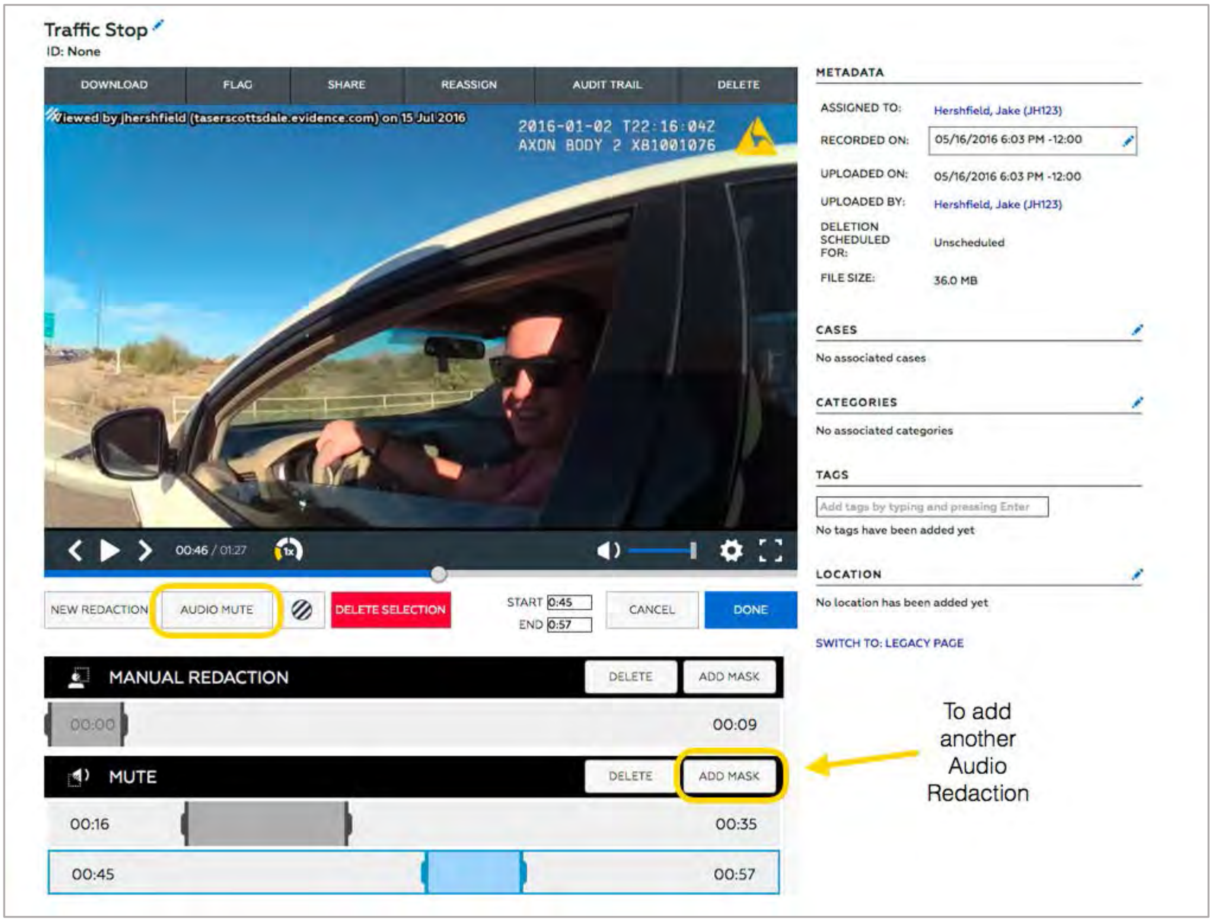
Keyboard Shortcuts

For users who redact a large volume of video, keyboard shortcuts are a simplified way to navigate throughout the video.

When selected on a redaction segment, the “A and S” keys move the start handle back and forth, respectively, and the left and right arrow keys move the end hand back and forth, respectively. These shortcuts allow users to complete frame-by-frame redaction in an intuitive way.

Audio Redaction

Users can redact audio just as they redact video, resulting in a complete removal of the audio track for the duration specified. Users can also redact the audio or different portions of the same video by pressing the “Add Mask” button.



Traffic Stop

ID: None

Viewed by jhershfield (taserscottsdale.evidence.com) on 15 Jul 2016

2016-01-02 T22:16:04Z
AXON BODY 2 X81001076

00:46 / 01:27

START 0:45
END 0:57

METADATA

ASSIGNED TO:	Hershfield, Jake (JH123)
RECORDED ON:	05/16/2016 6:03 PM -12:00
UPLOADED ON:	05/16/2016 6:03 PM -12:00
UPLOADED BY:	Hershfield, Jake (JH123)
DELETION SCHEDULED FOR:	Unscheduled
FILE SIZE:	36.0 MB

CASES

No associated cases

CATEGORIES

No associated categories

TAGS

Add tags by typing and pressing Enter

No tags have been added yet

LOCATION

No location has been added yet

SWITCH TO: LEGACY PAGE

MANUAL REDACTION: 00:00 – 00:09

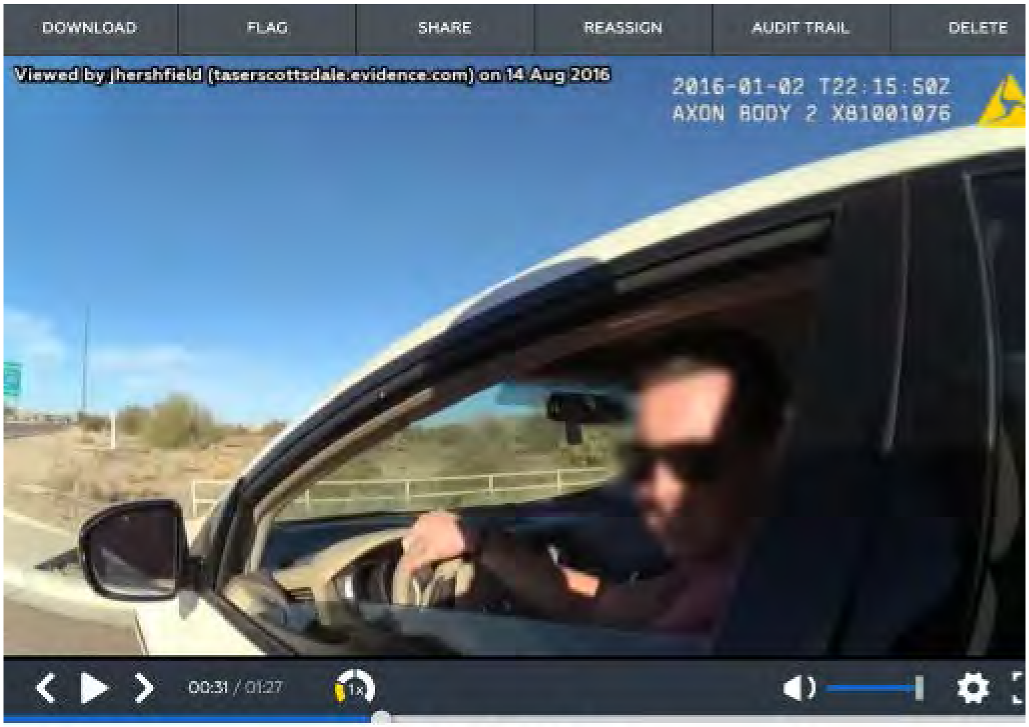
MUTE: 00:16 – 00:35; 00:45 – 00:57

To add another Audio Redaction

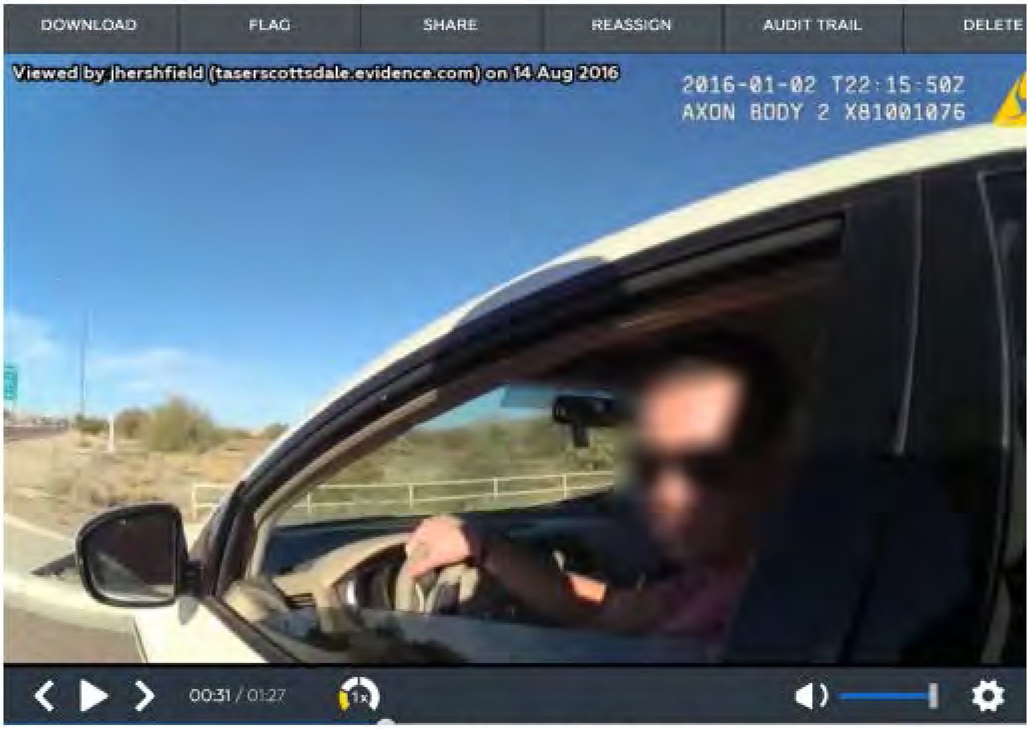
Filters

Evidence.com offers complete application of various image-processing filters for the duration specified. Optionally audio redaction can be enabled during video segments that have been blackout redacted. Examples of filters are as follows:

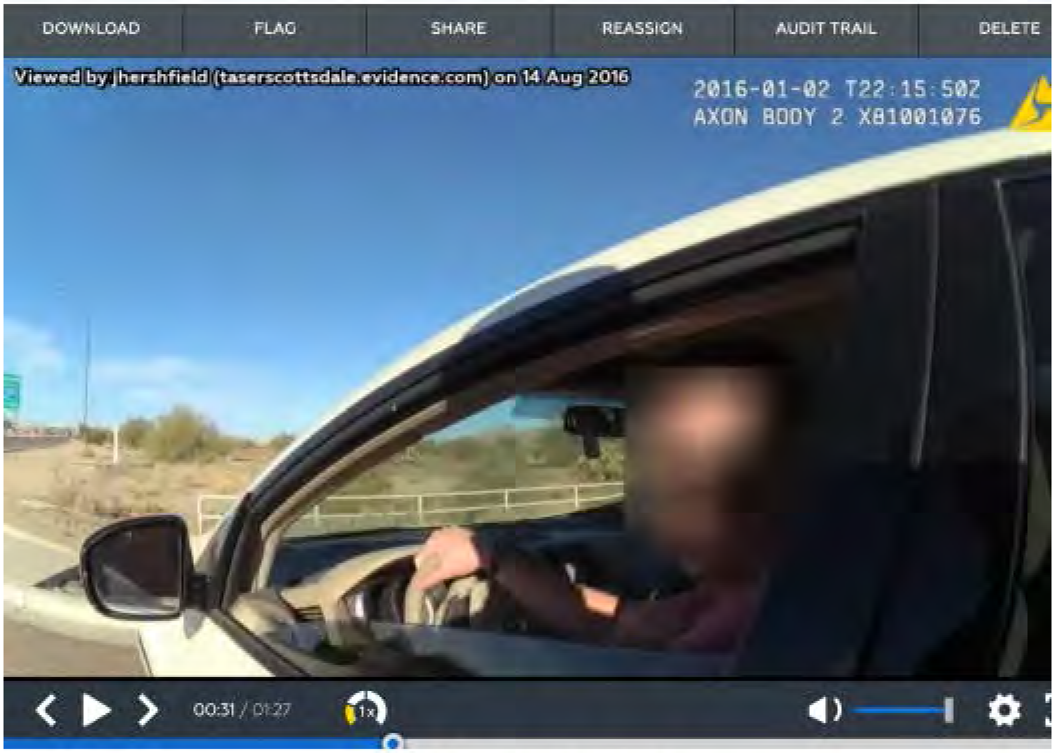
- Light Blur
- Normal Blur
- Heavy Blur
- Blackout



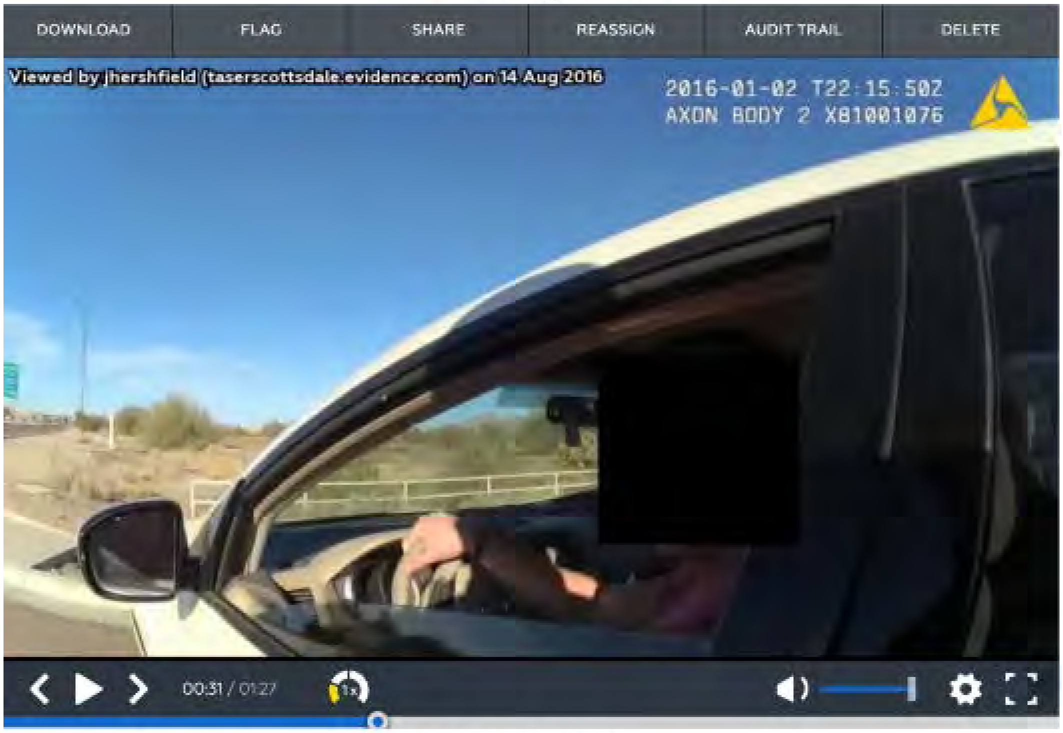
Light Blur



Normal Blur



Heavy Blur



Blackout

AXON

Evidence.com Administrator Reference Guide

Evidence.com August 2016 Release
Evidence.com Version 2016.8
Document Revision: A

Table of Contents

What’s New

No changes were made to this guide in support of Evidence.com August 2016. For more information about this release, see the Evidence.com August 2016 Release Notes.

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

Introduction

TASER International, Inc. (TASER) 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.io.

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

Capture

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

Transport

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

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

Data Management

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

About This Guide

This document is a reference for implementing the Evidence.com solution. The intended audience is primarily Evidence.com agency administrators, to assist with set-up of your Evidence.com agency and with the on-going operation of your agency. If you require additional assistance, contact Customer Service via help@evidence.com or at 800-978-2737 or +1 480-463-2170.

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—LITE or PRO.

- Confirm administrator status in Evidence.com
- Configure custom Roles and Permissions (optional)
- Configure and add users
- Configure account settings
- Confirm agency profile information
- Confirm camera settings (only applicable for Axon customers)
- Configure Fields & Retention Categories
- Enable IP address security (optional)
- Enable dual-factor authentication (optional)
- Configure password settings (optional)

Administrator Overview

For every agency on Evidence.com, during the initial implementation cycle, TASER creates an administrator account. 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.

Supported Web Browsers

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

- Internet Explorer version 10 and above

  Note: If you use Internet Explorer, ensure that Compatibility View is *disabled*. Evidence.com does not support the use of the Compatibility View feature. To verify your Internet Explorer settings, go to Tools > Compatibility View settings and ensure that Evidence.com is not included in the list of websites added to Compatibility View and that the "Display all websites in Compatibility View" check box is cleared.

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

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

- Internet Explorer version 10 and above
- Chrome version 43 and above
- Firefox version 38 and above
- Safari version 8 and above

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

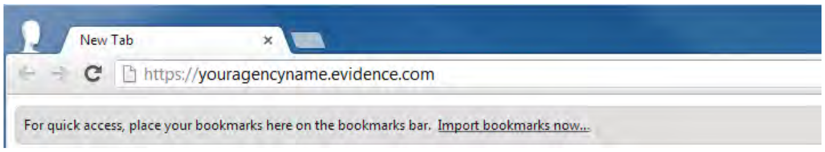
It is strongly recommended that you always use the latest release of Adobe Flash.

Sign In to Evidence.com

If you do not know your agency URL or are unsure if TASER has created an agency for you, contact TASER Customer Service at 1-800-978-2737 or your TASER sales engineer.

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

   `https://`*youragencyname*`.evidence.com`



New Tab

https://youragencyname.evidence.com

For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

Your agency's sign in page appears.

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

3. Click **Sign In**.

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

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

Dashboard

The Dashboard appears when you sign in to your Evidence.com agency. The Dashboard includes the following sections:

- System Alerts
- Critical Device Alerts
- Groups I Monitor
- Upcoming Evidence Deletions — User Initiated and System Initiated
- System Usage
- My Latest Uploads
- Evidence Shared with Me
- My Case Activity

Viewing the Dashboard

The Dashboard appears when you sign in to your Evidence.com agency.

To open the Dashboard page when you have already signed in to Evidence.com, click the Axon logo: ⚠

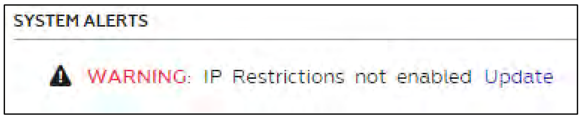
System Alerts

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

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

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

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



SYSTEM ALERTS

⚠ WARNING: IP Restrictions not enabled Update

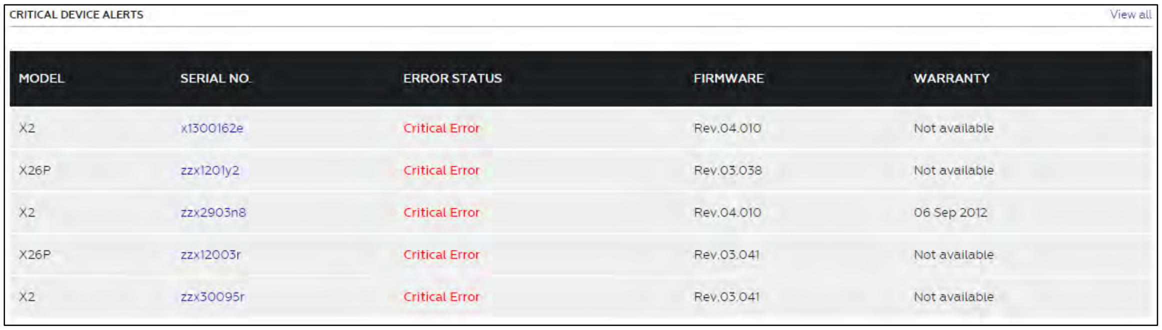
Critical Device Alerts

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

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

If none of your agency's TASER devices have a critical error status, "No Results Found" appears in this section.

If you want to see all devices that have an error status of Critical, in the upper-right corner of the Critical Device Alerts section, click **View all**.



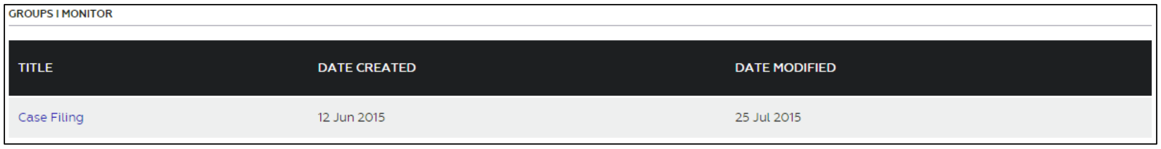
CRITICAL DEVICE ALERTS

View all

MODEL	SERIAL NO.	ERROR STATUS	FIRMWARE	WARRANTY
X2	x1300162e	Critical Error	Rev.04.010	Not available
X26P	zzx1201y2	Critical Error	Rev.03.038	Not available
X2	zzx2903n8	Critical Error	Rev.04.010	06 Sep 2012
X26P	zzx12003r	Critical Error	Rev.03.041	Not available
X2	zzx30095r	Critical Error	Rev.03.041	Not available

Groups I Monitor

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



GROUPS I MONITOR

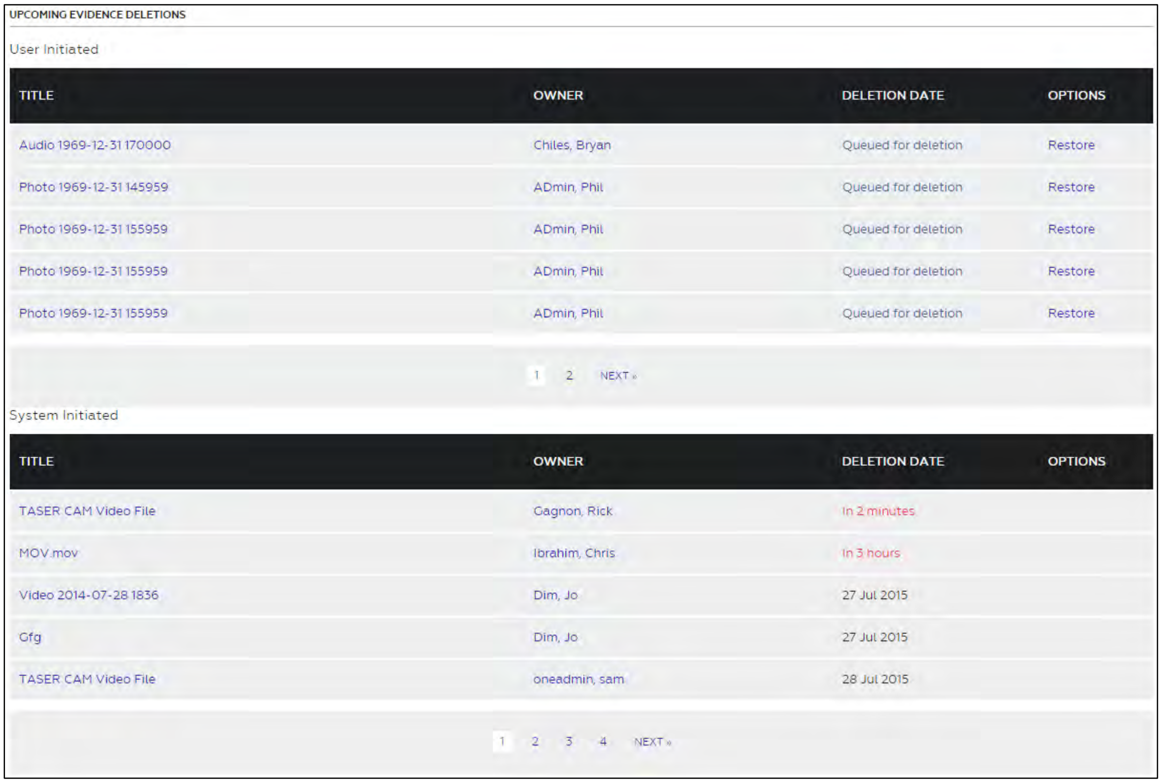
TITLE	DATE CREATED	DATE MODIFIED
Case Filing	12 Jun 2015	25 Jul 2015

Upcoming Evidence Deletions

The Upcoming Evidence Deletions section includes two lists:

- User Initiated — Lists evidence that has been manually scheduled for deletion.
- System Initiated — Lists evidence automatically scheduled for deletion in accordance with the retention duration of the category that is assigned the evidence. For more information, see Categories and Evidence Retention Policies.

Each list shows five evidence files at a time. To move through a list, use the pagination controls below the list.



UPCOMING EVIDENCE DELETIONS

User Initiated

TITLE	OWNER	DELETION DATE	OPTIONS
Audio 1969-12-31 170000	Chiles, Bryan	Queued for deletion	Restore
Photo 1969-12-31 145959	ADmin, Phil	Queued for deletion	Restore
Photo 1969-12-31 155959	ADmin, Phil	Queued for deletion	Restore
Photo 1969-12-31 155959	ADmin, Phil	Queued for deletion	Restore
Photo 1969-12-31 155959	ADmin, Phil	Queued for deletion	Restore

1 2 NEXT »

System Initiated

TITLE	OWNER	DELETION DATE	OPTIONS
TASER CAM Video File	Gagnon, Rick	In 2 minutes	
MOV.mov	Ibrahim, Chris	In 3 hours	
Video 2014-07-28 1836	Dim, Jo	27 Jul 2015	
Cfg	Dim, Jo	27 Jul 2015	
TASER CAM Video File	oneadmin, sam	28 Jul 2015	

1 2 3 4 NEXT »

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

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

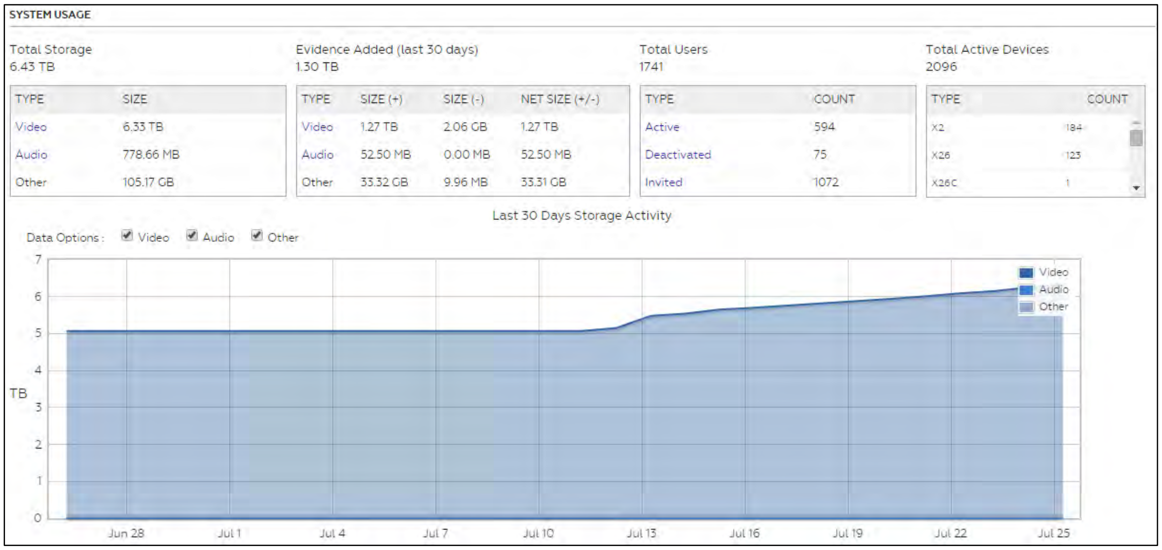
- To restore evidence from the User Initiated list, click **Restore** and then, on the confirmation message box, click **OK**.
- To restore evidence from the System Initiated list, click the evidence title and then assign the evidence a category with a retention duration that prevents the deletion of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

System Usage

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

It displays the amount of evidence added and deleted by your agency's users as well the average (net) in the last 30 days.

It also displays the total number of Evidence.com users and your agency's active TASER devices.



SYSTEM USAGE

Total Storage
6.43 TB

TYPE	SIZE
Video	6.33 TB
Audio	778.66 MB
Other	105.17 GB

Evidence Added (last 30 days)
1.30 TB

TYPE	SIZE (+)	SIZE (-)	NET SIZE (+/-)
Video	1.27 TB	2.06 GB	1.27 TB
Audio	52.50 MB	0.00 MB	52.50 MB
Other	33.32 GB	9.96 MB	33.31 GB

Total Users
1741

TYPE	COUNT
Active	594
Deactivated	75
Invited	1072

Total Active Devices
2096

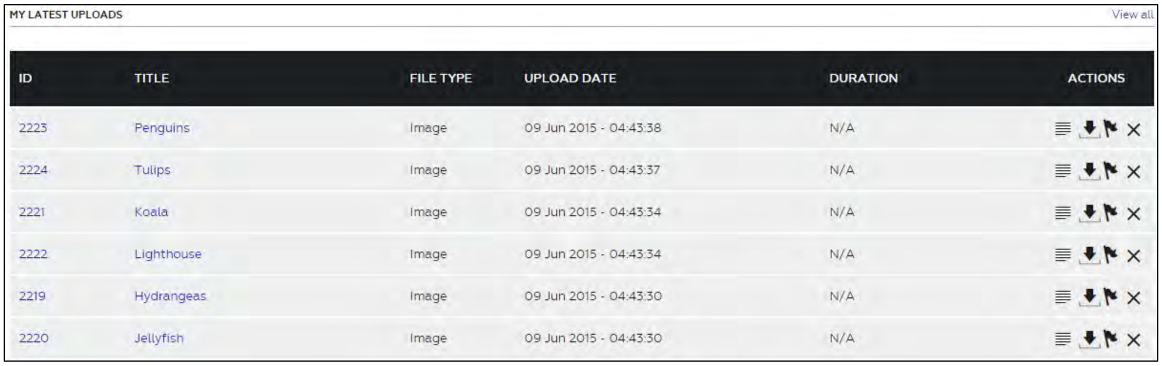
TYPE	COUNT
X2	184
X26	123
X26C	1

Last 30 Days Storage Activity

Data Options : ☑ Video ☑ Audio ☑ Other

My Latest Uploads

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



MY LATEST UPLOADS

View all

ID	TITLE	FILE TYPE	UPLOAD DATE	DURATION	ACTIONS
2223	Penguins	Image	09 Jun 2015 - 04:43:38	N/A	≣ ⬇ ⚑ ✕
2224	Tulips	Image	09 Jun 2015 - 04:43:37	N/A	≣ ⬇ ⚑ ✕
2221	Koala	Image	09 Jun 2015 - 04:43:34	N/A	≣ ⬇ ⚑ ✕
2222	Lighthouse	Image	09 Jun 2015 - 04:43:34	N/A	≣ ⬇ ⚑ ✕
2219	Hydrangeas	Image	09 Jun 2015 - 04:43:30	N/A	≣ ⬇ ⚑ ✕
2220	Jellyfish	Image	09 Jun 2015 - 04:43:30	N/A	≣ ⬇ ⚑ ✕

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

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

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

Under Actions, you can view the evidence audit trail, download the evidence, flag the evidence, or delete the evidence.

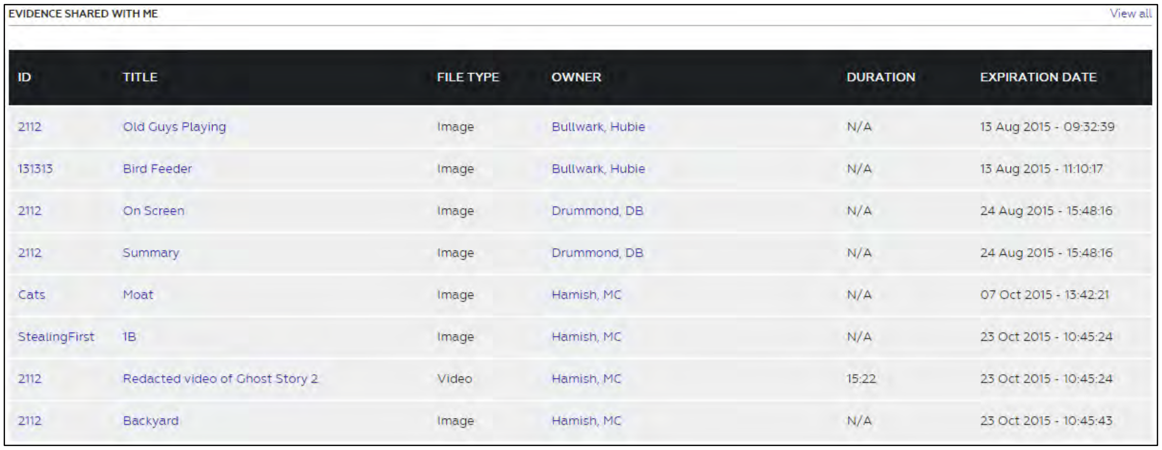
Evidence Shared with Me

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

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

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

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



EVIDENCE SHARED WITH ME

ID	TITLE	FILE TYPE	OWNER	DURATION	EXPIRATION DATE
2112	Old Guys Playing	Image	Bullwark, Hubie	N/A	13 Aug 2015 - 09:32:39
131313	Bird Feeder	Image	Bullwark, Hubie	N/A	13 Aug 2015 - 11:10:17
2112	On Screen	Image	Drummond, DB	N/A	24 Aug 2015 - 15:48:16
2112	Summary	Image	Drummond, DB	N/A	24 Aug 2015 - 15:48:16
Cats	Moat	Image	Hamish, MC	N/A	07 Oct 2015 - 13:42:21
StealingFirst	1B	Image	Hamish, MC	N/A	23 Oct 2015 - 10:45:24
2112	Redacted video of Ghost Story 2	Video	Hamish, MC	15:22	23 Oct 2015 - 10:45:24
2112	Backyard	Image	Hamish, MC	N/A	23 Oct 2015 - 10:45:43

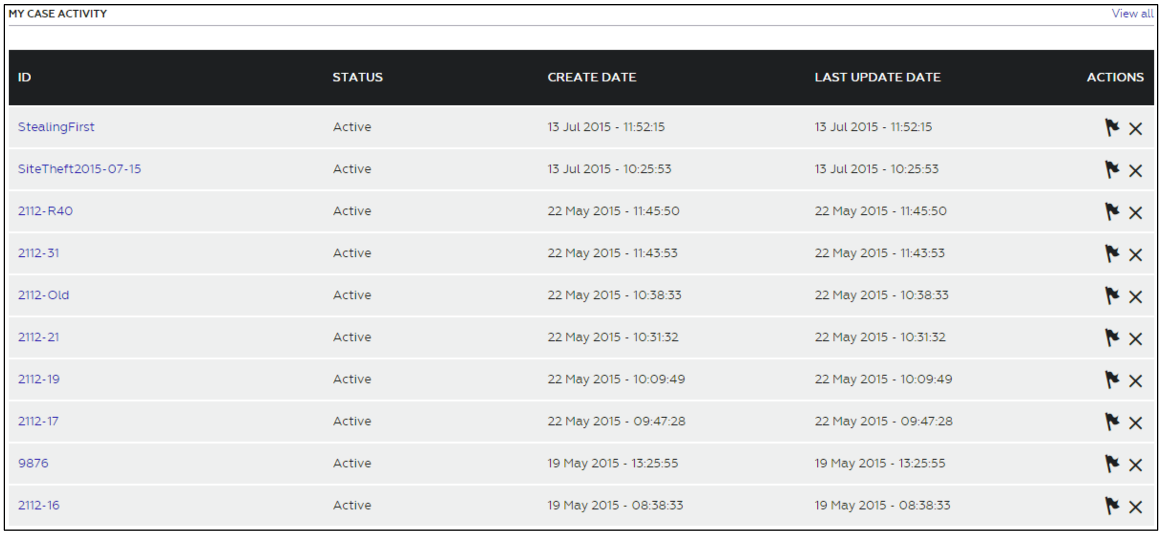
My Case Activity

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

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

If you want to view the details of a case, click the case ID.

Under Actions, you can flag cases or delete them.



MY CASE ACTIVITY

ID	STATUS	CREATE DATE	LAST UPDATE DATE	ACTIONS
StealingFirst	Active	13 Jul 2015 - 11:52:15	13 Jul 2015 - 11:52:15	⚑ ✕
SiteTheft2015-07-15	Active	13 Jul 2015 - 10:25:53	13 Jul 2015 - 10:25:53	⚑ ✕
2112-R40	Active	22 May 2015 - 11:45:50	22 May 2015 - 11:45:50	⚑ ✕
2112-31	Active	22 May 2015 - 11:43:53	22 May 2015 - 11:43:53	⚑ ✕
2112-Old	Active	22 May 2015 - 10:38:33	22 May 2015 - 10:38:33	⚑ ✕
2112-21	Active	22 May 2015 - 10:31:32	22 May 2015 - 10:31:32	⚑ ✕
2112-19	Active	22 May 2015 - 10:09:49	22 May 2015 - 10:09:49	⚑ ✕
2112-17	Active	22 May 2015 - 09:47:28	22 May 2015 - 09:47:28	⚑ ✕
9876	Active	19 May 2015 - 13:25:55	19 May 2015 - 13:25:55	⚑ ✕
2112-16	Active	19 May 2015 - 08:38:33	19 May 2015 - 08:38:33	⚑ ✕

User Administration

An administrator or a user allowed the User Administration permission generates all user accounts in your Evidence.com agency. When you add a user to your Evidence.com agency, Evidence.com sends an invitation to the email address of the user.

Please note the following requirements and best practices:

- All users in your Evidence.com agency must have unique email accounts.
- Users must have access to their email accounts.
- Each user should have a unique Evidence.com account. It is recommended that you prohibit users from sharing an Evidence.com user account.
- If you do not want to allow users to change their username, email address, or other information, ensure that the role that you assign to users prohibits the Edit Account Information permission.

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

- Invitations to register with Evidence.com are valid for seven days. If the user fails to register within that span of time, an administrator must re-invite them.
- In order to avoid complications later, it is recommended that you create a policy that dictates username format.

After users have registered in Evidence.com, they can log in to Evidence.com.

User Account Statuses

An Evidence.com user account can have one of the following possible statuses.

- **Active** — The user can access your Evidence.com agency, as determined by the role that you assigned to the user account. Administrators can change user account information for Active users.

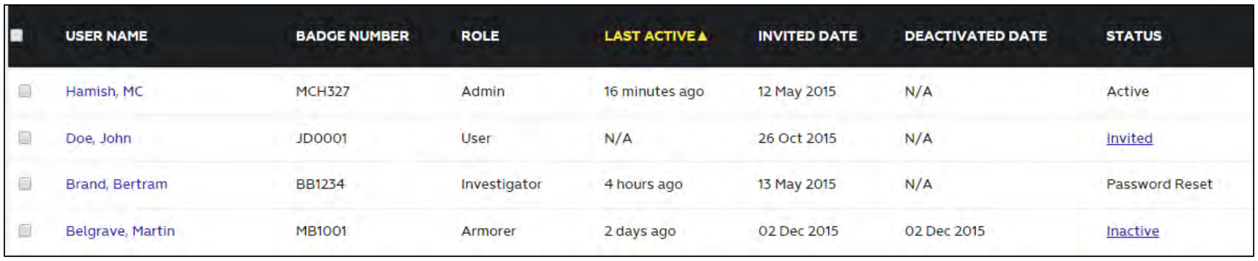
  Evidence.com does not permit users who have not completed the registration process to access your Evidence.com agency.

- **Invited** — Active users who have not completed the registration process are considered to have a status of Active/Invited. In user search results, the status of these users is listed as Invited.

- **Password Reset** — Active users whose credentials have been reset by an administrator have a status of Active/Password Reset. In user search results, the status of these users is listed as Password Reset.
- **Inactive** — The user cannot access your Evidence.com agency. Administrators cannot change user account information for Inactive users; however, the audit trails of inactive users remain available.

  Administrators can create user accounts that are Inactive. This enables agencies to pre-provision user accounts with device assignments and other settings, without prematurely allowing the users access to their Evidence.com agency.

The following figure shows user search results that contain user accounts in each of the possible statuses, as shown by the far right column.



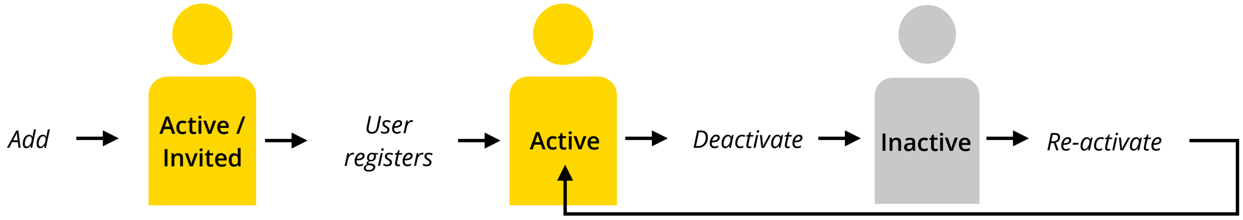
☐	USER NAME	BADGE NUMBER	ROLE	LAST ACTIVE ▲	INVITED DATE	DEACTIVATED DATE	STATUS
☐	Hamish, MC	MCH327	Admin	16 minutes ago	12 May 2015	N/A	Active
☐	Doe, John	JD0001	User	N/A	26 Oct 2015	N/A	Invited
☐	Brand, Bertram	BB1234	Investigator	4 hours ago	13 May 2015	N/A	Password Reset
☐	Belgrave, Martin	MB1001	Armorer	2 days ago	02 Dec 2015	02 Dec 2015	Inactive

You cannot delete user accounts. This ensures that user audit trails are available any user accounts 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.

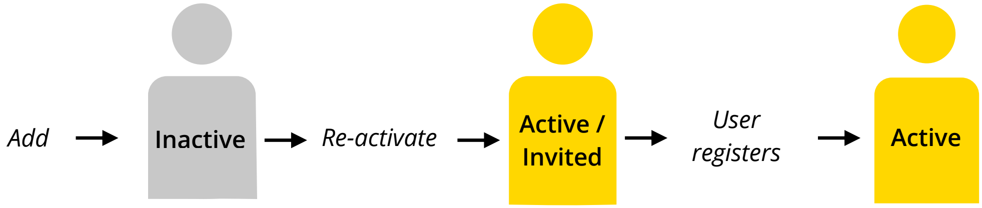
User Account Added as Active

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.



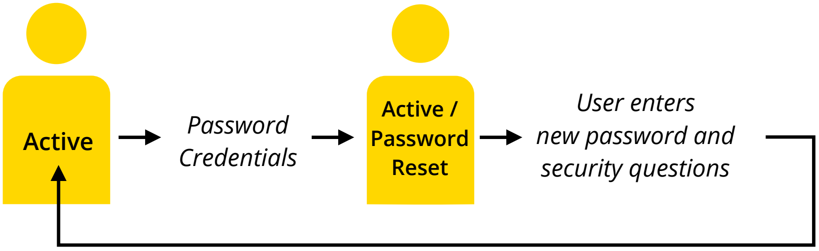
User Account Added as Inactive

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 under **Users**, click **Add User**.

   The Add User page appears.

2. In the following boxes, type the required information.

   - **First Name** — The user's first name.
   - **Last Name** — The user's last name.
   - **Email Address** — The unique Internet email address of the user.
   - **Username** — A unique username that you assign.
   - **Badge Number** — 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. For more information, see the axon.io/cad-rms web site.

3. In the **User role** list, click the role that you want to assign to the user.

4. In the **Status** list, click the status that you want to the user.

   - **Active** — The user is able to register and sign in to Evidence.com immediately after you finish adding the user.
   - **Inactive** — The user is not able to register or sign in to Evidence.com.

5. Click **Add**.

   Evidence.com adds the user. If the user status is Active, Evidence.com sends the user an invitation email.

   A notification message box appears.

6. On the message box, click the button for the action you want to take next.

Add Many Users

When you need to add many users to your Evidence.com agency, use the Import Users feature. This feature lets you create many user accounts quickly. You specify details about the new users in a file that you upload to Evidence.com.

You are limited to assigning the same user role to each user that you add from an uploaded file; therefore, create upload files that contain only users that you want to assign to the same user role. For example, create an upload file for users that you want to assign the Armorer role and create a different upload file for users that you want to assign the User role.

The supported file formats are the following formats:

- Comma-separated values (CSV) file — Supported by spreadsheet applications, such as Microsoft Excel.
- Text (TXT) file — Supported by text editors and word processors. It is recommended that you use a text editor such as Microsoft Notepad to ensure that the file format is correct.

In either format, you must specify the following information for each user:

- First name
- Last name
- Email address
- Badge ID
- Username
- Status

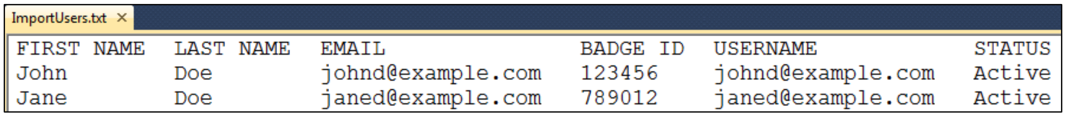
Note: In order to complete the registration process, users must have access to the email addresses that you specify.

1. On the menu bar, click **Admin** and then under **Users**, click **Import Users**.

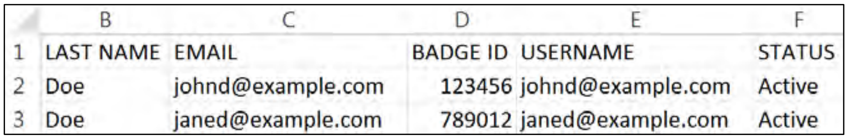
   The Import Users page appears.

2. Download the example file for the format that you want to use.
3. Make a copy of the example file and assign it a meaningful file name.
4. Open the file in the appropriate application. For a .txt file, use a text editor. For a .csv file, use a spreadsheet application.

The first row or line of the file contains column names. The second and third row or line is an example.



```
FIRST NAME   LAST NAME   EMAIL                 BADGE ID   USERNAME              STATUS
John         Doe         johnd@example.com     123456     johnd@example.com     Active
Jane         Doe         janed@example.com     789012     janed@example.com     Active
```



	B	C	D	E	F
1	LAST NAME	EMAIL	BADGE ID	USERNAME	STATUS
2	Doe	johnd@example.com	123456	johnd@example.com	Active
3	Doe	janed@example.com	789012	janed@example.com	Active

5. Delete the second and third lines. *Do not* delete the first line. Evidence.com expects the first line to contain the column names.

6. For every user that you want to add, include a line in the file that specifies values for the user first name, last name, email address, and badge ID.

   Ensure that you separate the values in each row or line appropriately:

   - In a .txt file, ensure that you add a tab after each value.

   - In a .csv file, ensure that each value is in the cell beneath the applicable header.

7. Save the file.

8. In Evidence.com, if your session has timed out, sign in again and return to the Import Users page by clicking **Admin** and then, under **Users**, clicking **Import Users**.

9. Click **Choose File** and, in the dialog box that opens, select the file on your computer, and then click **Next**.

   Evidence.com displays a list of the users found in the uploaded file.

10. For each user that you want to add, select the check box to the left of the user first name.

11. In the **Role for all users** list, click the user role that you want to assign to each user that you selected and then click **Next**.

    Evidence.com displays a confirmation page. The role to be assigned to each user is noted near the bottom of the page.

12. Review the user information a final time and then click **Next**.

    Evidence.com imports the users and sends each user an invitation email.

A message box displays buttons for importing more users or ending the process.

13. Click the button for the action you want to take next.

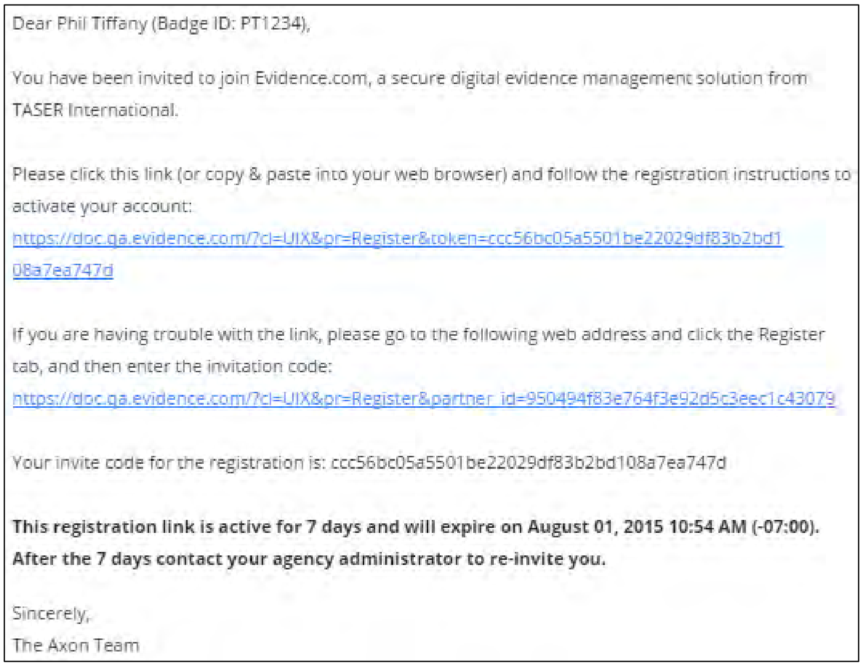
Complete the User Registration Process

In order to access your Evidence.com agency, users who have received an invitation email must register with Evidence.com. Users must have to 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 TASER devices to their agency's Active users who have not yet registered on Evidence.com.

1. Locate the invitation email that Evidence.com sent to the address entered by your administrator while creating your Evidence.com user account.



Dear Phil Tiffany (Badge ID: PT1234),

You have been invited to join Evidence.com, a secure digital evidence management solution from TASER International.

Please click this link (or copy & paste into your web browser) and follow the registration instructions to activate your account:
https://doc.qa.evidence.com/?cl=UIX&pr=Register&token=ccc56bc05a5501be22029df83b2bd108a7ea747d

If you are having trouble with the link, please go to the following web address and click the Register tab, and then enter the invitation code:
https://doc.qa.evidence.com/?cl=UIX&pr=Register&partner_id=950494f83e764f3e92d5c3eec1c43079

Your invite code for the registration is: ccc56bc05a5501be22029df83b2bd108a7ea747d

This registration link is active for 7 days and will expire on August 01, 2015 10:54 AM (-07:00). After the 7 days contact your agency administrator to re-invite you.

Sincerely,
The Axon Team

2. Click the first link in the email.

   Your default web browser opens your Evidence.com agency Registration page.

   Note: Alternately, in the email, copy the invite code and then click the second link. After the registration page opens, paste the invite code and click OK.

3. Complete the registration form.

4. Review End User License Agreement (EULA) and select the **EULA Confirmation** checkbox.

5. Click **Submit**.

   Evidence.com sends you a welcome email.

Re-Invite Users

Invitations to join Evidence.com expire within 7 days. After an invitation expires, an agency administrator can re-invite the user.

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.

   The All Users page lists all users in your agency. The row of buttons below the search filters includes a Reinvite Users button.

2. In the **Status** list, click **Active/Invited**, and then click **Search**.

   Evidence.com lists users whose status is Active but who have not yet completed user registration.

3. For each user you want to re-invite, select the check box next the user name.

4. Click **Reinvite Users**.

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

   Evidence.com sends the selected users a new invitation email.

Deactivate Users

You can deactivate user accounts that have a status of Active. Evidence.com does not allow a user with a deactivated account to sign in.

When you deactivate a user account, the status of the user account is Inactive. Evidence.com sends the user an email stating that the account is deactivated.

You can deactivate users in two ways:

- Many users at once, from user-search results.
- One user at a time, from a User Summary page.

Deactivate Many Users

From a user search page, you can deactivate more than one user account at a time.

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.

   The All Users page lists all users in your agency. The row of buttons below the search filters includes the Deactivate Users button.

2. In the **Status** list, click **Active**, and then click **Search**.

   Evidence.com lists users whose status is Active.

3. If you need to refine the search results more, use the search filters as needed.

4. For each user you want to deactivate, select the check box to the left of the user name. If you want to deactivate all users shown in search results, select the check box at the top left of the search results.

5. Click **Deactivate Users**.

   A dialog box for reassigning the users' evidence and devices appears. By default, the "Evidence Files and Devices Remain Assigned to the Current User" option is selected.

6. If you do *not* want to reassign the users' evidence and devices, skip to step 10.

7. If you want to reassign the users' evidence and devices, click **Reassign the Evidence and Devices to Another User**.

8. In the **Reassign to** box, start typing the name of the user to whom you want to reassign evidence and devices. The user must belong to the same agency as the users whom you are deactivating.

   Evidence.com shows a list of users that match what you have typed.

9. Click the user to whom you want to reassign evidence and devices.

10. Click **Deactivate User**.

11. On the notification message box stating how many user accounts you deactivated, click **OK**.

    Evidence.com sends a notification email to each user whose account you deactivated.

    Because the User Results page does not automatically update, the user statuses continue to show as Active.

12. If you want to confirm that the accounts are deactivated, search for the users again.

Deactivate One User

From the User Summary page, you can deactivate a single user.

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.

   The All Users page lists all users in your agency.

2. Search for the active user whose account you want to deactivate.

3. In the user search results, click the user name.

   The User Summary page appears.

4. Click **Manage User**.

   The User Information page appears.

5. Click **Deactivate User**.

   A dialog box for reassigning the user's evidence and devices appears. By default, the "Evidence Files and Devices Remain Assigned to the Current User" option is selected.

6. If you do *not* want to reassign the user's evidence and devices, skip to step 10.

7. If you want to reassign the user's evidence and devices, click **Reassign the Evidence and Devices to Another User**.

8. In the **Reassign to** box, start typing the name of the user to whom you want to reassign evidence and devices. The user must belong to the same agency as the user whom you are deactivating.

   Evidence.com shows a list of users that match what you have typed.

9. Click the user to whom you want to reassign evidence and devices.

10. Click **Deactivate User**.

11. On the notification message box states that the user account has been deactivated, click **OK**.

    Account details for the deactivated user appear.

    Evidence.com sends a notification email to the user whose account you deactivated.

Reactivate Users

Agency administrators can reactivate previously deactivated users.

You can reactivate user accounts that have a status of Inactive.

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.
2. In the **Status** list, click **Deactivated**, and then click **Search**.

   Evidence.com lists users whose status is Inactive.
3. If you need to refine the search results more, use the search filters as needed.
4. For each user you want to reactivate, select the check box to the left of the user name. If you want to reactivate all users shown in search results, select the check box at the top left of the search results.
5. Click **Reactivate Users**.

   Note: You can reactivate a single user by clicking Deactivated under Status in the user's row.
6. On the confirmation message box, click **OK**.
7. On the notification message box, click **OK**.

   Evidence.com sends each user an email stating that the user's account active again.

   Because the User Results page does not automatically update, the user statuses continue to show as Deactivated.
8. If you want to confirm that the accounts are active, search for the users again.

Unlock a User Account

When a user attempts and fails to sign in to Evidence.com more times than are allowed by the agency's security settings, the user is locked out of Evidence.com and receives the message, "Too many failed login attempts. Account temporarily suspended."

You can unlock user accounts that are locked.

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.

   The All Users page lists all users in your agency.

2. Search for the user whose account you want to unlock.

   User search results do *not* show whether an account is locked.

3. In the user search results, click the user name.

   The User Summary page appears.

4. Click **Manage User**.

   If the account is locked, the Unlock Account button is available.

5. Click **Unlock Account**.

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

   The user account is unlocked, the page refreshes, and the Unlock Account button is not available.

Reset Passwords and Security Questions

When you reset a user's password and security questions, Evidence.com sends the user an email with information about the change and a temporary password that allows the user to sign in, change the password, and specify new security questions.

Reset Password and Security Questions from a User Details Page

You can reset the password and security questions of a single user from the User Details page.

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.

   The All Users page lists all users in your agency.

2. Search for the user whose password and security questions you want to reset.

3. In the user search results, click the user name.

   The User Summary page appears.

4. Click **Manage User**.

   The User Details page appears.

5. Click **Reset Credentials**.

6. On the confirmation message box, click **Continue**.

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

   Evidence.com sends the user an email that explains that the user's password has been reset and provides instructions for creating a new password and security questions.

Reset Passwords and Security Questions for Users from User Search Results

From the results of a user search, you can reset the password of more than one user accounts at a time.

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.

   The All Users page lists all users in your agency.

2. Search for users and refine the search until the search results includes users whose passwords and security questions you want to reset.

3. For each user whose password you want to reset, select the check box to the left of the user name. If you want to reset passwords for all users shown in search results, select the check box at the top left of the search results.

4. Click **Reset Password**.

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

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

   Evidence.com sends each user an email that explains that the user's password has been reset and provides instructions for creating a new password and security questions.

Send a Message to a User

You can send a message to an active user.

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.

   The All Users page lists all users in your agency.

2. Search for the active user.

3. In the user search results, click the user name.

   The User Summary page appears. The Send Message button is below the basic user information.

4. Click **Send Message**.

   The Compose Message page appears.

5. In the **Subject** and **Message** boxes, type the subject and your message, and then click **Send**.

   Evidence.com sends the message to the user you specified.

Change a Username

Administrators can change the username of a user account, if the user account status is Active.

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.

   The All Users page lists all users in your agency.

2. Search for the user whose username you want to change.

3. In the user search results, click the user name.

   The User Summary page appears.

4. Click **Manage User**.

5. Under **Account Details**, in the **Username** box, change the username, as needed.

6. Click **Save**.

   Evidence.com sends the user an email, notifying them of the change.

   All changes are tracked in the user audit trail.

Edit Other User Account Information

From the User Details page, administrators can update basic user information such as username, first name, last name, badge ID, email address, user role, and time zone.

It is recommended that usernames and badge ID

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.

   The All Users page lists all users in your agency.

2. Search for the user whose details you want to edit.

3. In the user search results, click the user name.

   The User Summary page appears.

4. Click **Manage User**.

   The User Details page includes an Account Details area.

5. Update the Account Details section as needed and then click **Save**.

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

User Audit Trail

A user audit trail shows many of the activities taken by the user in addition to changes to the user account. User audit trails are available 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
- Extend evidence retention period
- Flag or un-flag evidence

- Share evidence internally (with users in your Evidence.com agency)
- Share evidence externally (with users outside your Evidence.com agency)
- Add or edit evidence tags
- Add or edit evidence description
- Add, edit, or remove evidence notes
- Reassign evidence
- Add evidence to a case
- Add a marker
- Download a marker
- Add a video clip
- Add video redaction

Case-related user actions that appear in user audit trails include the following:

- Create case
- Viewed case
- Add evidence to a case
- Remove evidence from a case
- Share case by download link
- Share case with partner agency
- Share case with user in your agency (add member to case)
- Download case
- Add or remove folder
- Add or edit categories assigned to case
- Edit case title
- Add or edit case description
- Add, edit, or delete case notes
- Add or remove case tags

Get a User Audit Trail

1. On the menu bar, click **Admin** and then under **Users**, click **All Users**.
2. Search for the user whose audit trail you want to view.
3. In the user search results, click the user name.

   The User Summary page appears.
4. Click **View Audit Trail**.

   A dialog box provides options for the date range and file type.
5. Under **Select Date Range**, do one of the following:
   - If you want to view the whole audit trail, select **View entire audit log**.
   - If you want to view a portion of the audit trail, select **View portion of audit log**, either specify a date in either or both the **From** or **To** boxes or click a shortcut for a date range, such as Yesterday.
6. Under **Select File Type**, click the file type that you want.

   Evidence.com downloads the user audit trail in the format you selected.
7. Save or view the audit trail file, as needed.

Expire All Passwords

An administrator can force agency-wide password resets.

1. On the menu bar, click **Admin** and then under **Security Settings**, click **Password Configuration**.
2. Under **Force Password Expiration for All Users**, click **Expire All Passwords**.
3. On the confirmation dialog box, click **Continue**.

   The next time each user signs in to your agency, Evidence.com requires that they change passwords.

Managing Your User Account

Users can update many settings for their own user accounts.

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

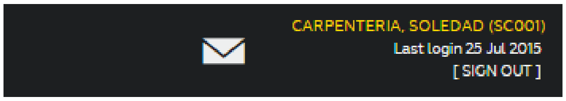
Note: The default permissions assigned to the User role does allow the Edit Account Information permission. For more information about permissions in pre-configured user roles, see Appendix A: Roles and Permissions.

Update Your Basic Account Information

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

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

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



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

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

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

3. Click **Save**.

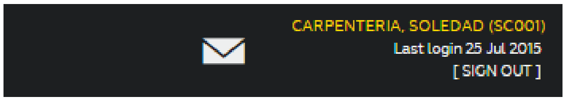
   Above User Information, a banner message about the success of the updates appears.

Verify Your Mobile Phone Number

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

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

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

   CARPENTERIA, SOLEDAD (SC001)
   Last login 25 Jul 2015
   [SIGN OUT]

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

2. Click **Send Verification Code**.

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

3. Click the button for the verification method you want to use.

   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.

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

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

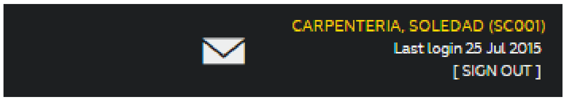
6. On the notification message box, click **OK**.

   Your mobile phone number is verified.

Change Your Password

You can change your password as needed.

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

   CARPENTERIA, SOLEDAD (SC001)
   Last login 25 Jul 2015
   [SIGN OUT]

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

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

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

3. Click **Save Password**.

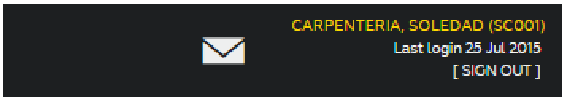
   Above Change Password, a banner message notifies you about the success of the password change.

Change Language

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

Note: If the language option is not available on the Accounts and Passwords page for your user account, then your organization has requested TASER to disable the feature for your Evidence.com agency.

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



CARPENTERIA, SOLEDAD (SC001)
Last login 25 Jul 2015
[SIGN OUT]

   The Account and Password page appears.

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

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

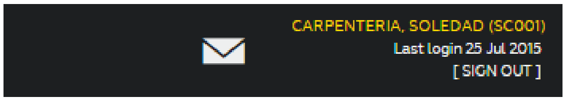
   The Evidence.com pages use the language that you selected.

Grant Temporary Access to TASER Customer Service

If you are experiencing any issues with Evidence.com account, TASER customer service may request temporary access to your user account for troubleshooting purposes. This feature enables TASER to access your agency using your user account in order to see the issue you are encountering.

Temporary access is revoked immediately when TASER customer service signs out of your user account.

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

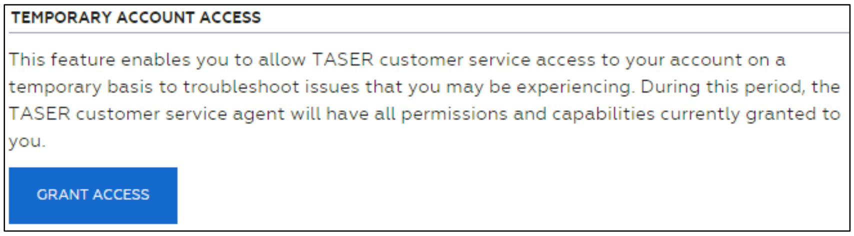


CARPENTERIA, SOLEDAD (SC001)
Last login 25 Jul 2015
[SIGN OUT]

The Account and Password page appears.

2. Under **Temporary Account Access**, click **Grant Access**.

To see the Temporary Account Access area, you may need to scroll to the bottom of the page.



TEMPORARY ACCOUNT ACCESS

This feature enables you to allow TASER customer service access to your account on a temporary basis to troubleshoot issues that you may be experiencing. During this period, the TASER customer service agent will have all permissions and capabilities currently granted to you.

GRANT ACCESS

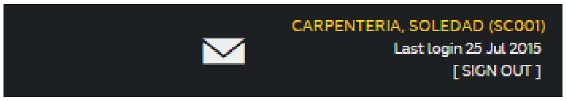
3. Review the warning message and then click **OK**.

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

Update Security Questions

You can update your security questions as needed.

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



CARPENTERIA, SOLEDAD (SC001)
Last login 25 Jul 2015
[SIGN OUT]

The Accounts and Passwords page appears.

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

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

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

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

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

5. Click **Save** and then, on the notification message box, click **OK**.

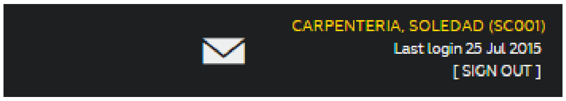
Update Your Email Notifications

You can set personal preferences for email notifications. The email notifications that are available to you are determined by the role assigned to your user account.

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.
- **Upcoming Evidence Deletion Notification** — Turn on to receive an email about the upcoming evidence deletions summary for the next week in your Evidence.com Inbox.
- **Evidence Timestamp 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.

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



The Accounts and Passwords page appears.

2. On the second menu bar, click **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 **Turn On** or **Turn Off**, as needed.

Groups Administration

The Groups feature provides 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.

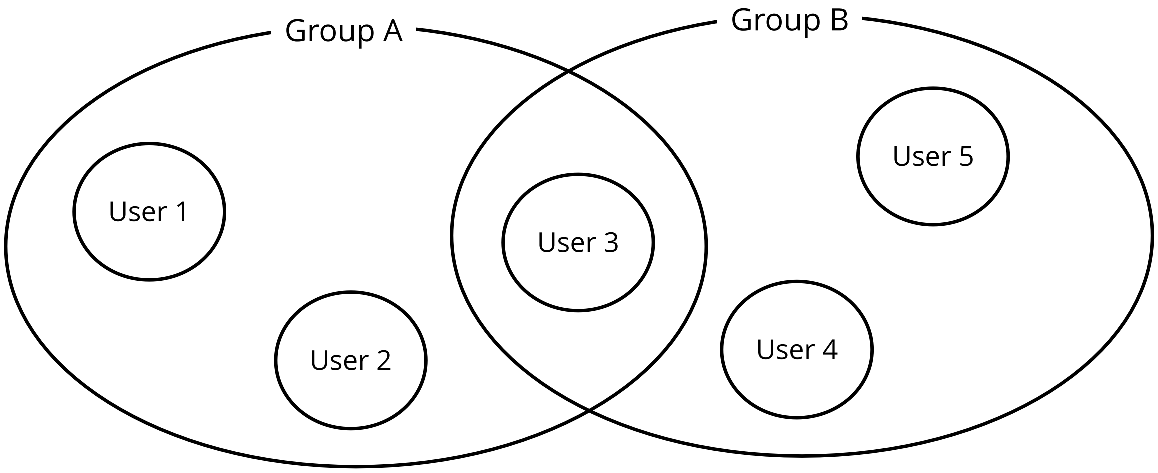
The Groups feature complements the Roles and Permissions feature. Unit leaders no longer must be granted permission to view all evidence of your agency, and you should remove this permission from leaders when you implement the Groups feature.

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 and has one or more members. Group members can be users, groups, or a mix of users and groups. Users and groups can be members or more than one group. There are no default groups.

The following figure shows two groups that each have three users. User 3 is a member of both groups.



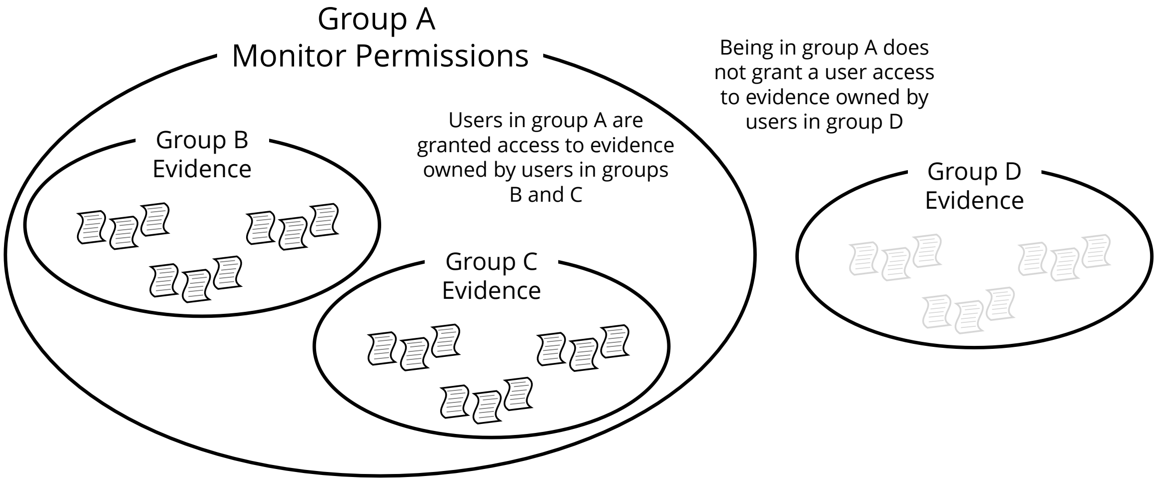
Monitoring Evidence with Groups

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, group A has permission to monitor the evidence owned by users in groups B and C.

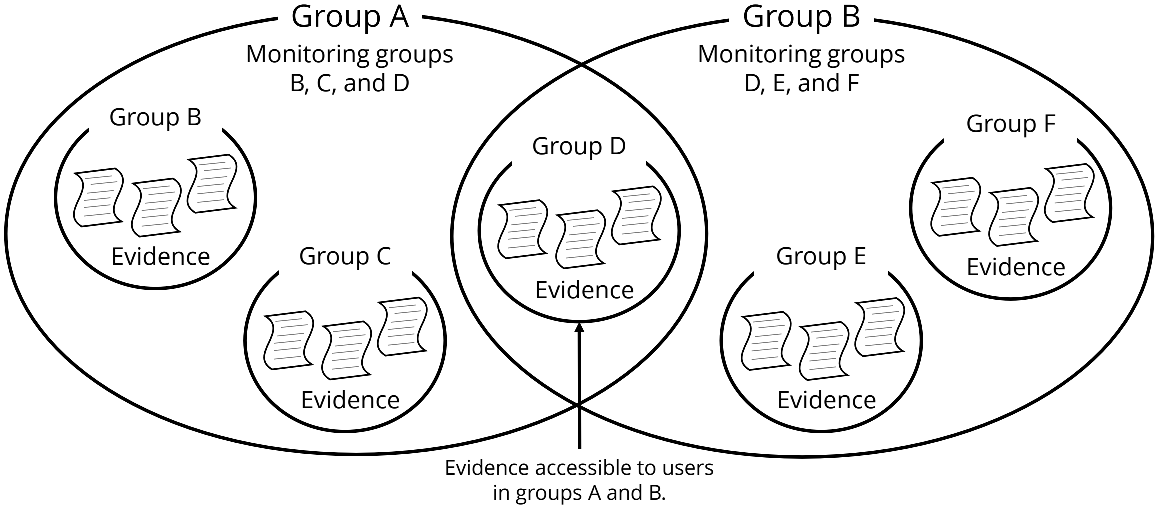

Group A
Monitor Permissions
Group B
Evidence
Users in group A are granted access to evidence owned by users in groups B and C
Group C
Evidence
Being in group A does not grant a user access to evidence owned by users in group D
Group D
Evidence

Note: In the preceding example, users who do not monitor Group D evidence but who are allowed the User Search permission can see Group D 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 A *and* B can:

- Monitor the evidence of users in groups B and C
- Have their evidence monitored by other users in group A.

More than one group can monitor the evidence of another group. In the following figure, groups A and B have permission to monitor the evidence of group D.



Groups Receiving Shared Cases from Partner Agencies

You can enable a group to receive cases shared by partner agencies. When a partner agency shares a case, they can send it to groups that you have permitted to receive shared cases. All members and monitors of the group receive a message notifying them that the shared case is available. Evidence.com determines the case owner. 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.

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 a single group, 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.

Users whose evidence search results should not list evidence that they do not have permission to view should be prohibited the User Search permission. On the Configure Role page, under Search Access, the User Search permission includes the Prohibited option.

When you implement the Groups feature, you can rely on the ability of monitoring groups to view the evidence uploaded by members of the groups that they monitor.

For more information about editing permissions in a role, see Edit a Role.

Group Management and Audit Permissions

Users whose responsibilities include creating, updating, and deleting groups must be allowed permission to create and edit groups. On the Configure Role page, under User Account, the Create/Edit Group permission includes the Allowed option.

Users whose responsibilities include importing groups, members, and monitors must be allowed permission to change agency security settings. On the Configure Role page, under Admin Access, the Configure Agency Security Settings permission includes the Allowed option.

Users whose responsibilities include viewing group audit trails must be allowed permission to view the audit trails. On the Configure Role page, under User Account, the Group Audit Trail PDF permission includes the Allowed option.

For more information about editing permissions in a role, see Edit a Role.

Create a Group

Users with permission to create a group can do so as needed.

At a minimum, when you create a group, you specify the group title. You can also add users and other groups as members, specify evidence-monitoring permissions, and specify whether the group can receive shared evidence from partner agencies.

1. On the menu bar, click **Admin** and then under **Users**, click **Create Group**.

   The Create Group page appears.

2. In the group-title text box, type a meaningful name for the group and then click **Create Group**. The group title must be at least three characters long and can be a maximum of 128 characters long.

   Evidence.com creates the group.

   A summary of the group that you created replaces the Create Group panel.

   The Add Members panel becomes available.

3. For each user or group that you want to add to the group, in the **Add Members** box, start typing the name of the user or group, wait for Evidence.com to show the list of matching users or groups, click the user or group that you want, and then click **Add**.

   Note: If you want to remove a user from the member list, under Actions click **Delete**.

4. Click **Next**.

   The Add Monitors panel becomes available.

5. If you want to allow partner agencies to share cases with this group, under **Sharing Permissions**, select **Allow Partner Agencies to share with this group**.

6. For each user or group who need to monitor evidence owned by members of this group, in the **Monitors of This Group** box, start typing the name of the user or group, wait for Evidence.com to show the list of matching users or groups, click the user or group that you want, and then click **Add**.

   Note: If you want the evidence of a monitor to be visible to other monitors, add the monitor to the group as a member.

7. For each user or group whose evidence should be monitored by members of this group, in the **This Group Can Monitor** box, start typing the name of the user or group, wait for

Evidence.com to show the list of matching users or groups, click the user or group that you want, and then click **Add**.

8. Click **Done**.

   The Group Profile page shows the members and monitors of the group.

Import Groups, Members, and Monitors

Administrators and users allowed the Configure Agency Security Settings permission have a swift and scalable way to manage Evidence.com groups. The Import Groups feature lets you use comma-separated value (CSV) files to create groups and to define group members and monitors. The Import Groups feature is available on the Admin Portal page.

Import Groups provides separate processes for defining groups and for configuring group members and monitors. A different CSV file is required for each process. For more information about the CSV files, see Import Groups and Define Members and Monitors.

Strategies for Importing Groups, Members, and Monitors

It is recommended that you consider how your organization can best make use of the Import Groups feature.

Setup by Import, Maintain by Import

The primary use for the Import Groups feature is to enable agencies to keep their Evidence.com group configurations in sync with groups in other applications, such as with an on-premises Microsoft Active Directory implementation.

With this strategy, it is recommended that your groups CSV file and members-and-monitors CSV file reflect the complete configuration of all groups and their members and monitors. It is also recommended that you ensure that the CSV files are backed up reliably.

Setup by Import, Maintain Manually

If you have no need to synchronize group configuration with an external source, consider using the Import Groups feature when you are setting up groups for the first time. Rather than creating groups one at a time, you can define the groups and their members and monitors using CSV files, and then import the files.

After importing groups and defining members and monitors, you can review your group configuration in Evidence.com and update it as needed. If a large number of changes are needed, it is likely more efficient to update the CSV files and reimport them.

When you are satisfied with your initial group configuration, you can begin maintaining groups individually, as described in Edit Group Members, Monitors, and Other Settings.

Empty Groups

You cannot use the Define Members and Monitors feature to empty an existing group of all members and monitors. It is recommended that you delete a group rather than trying to maintain an empty group. You can always create the group again later, when it is needed.

Import Groups

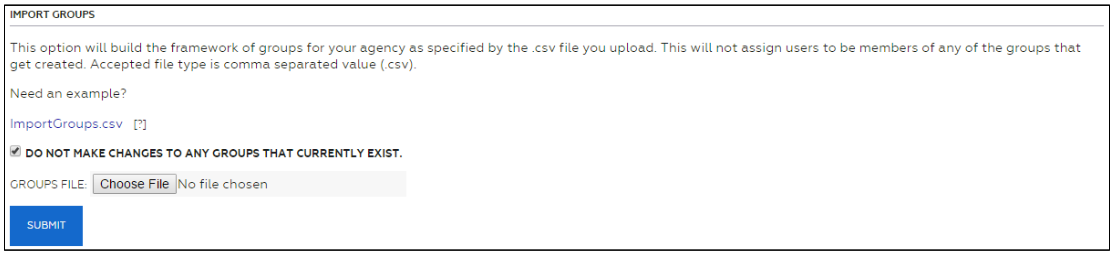
The CSV file for importing groups must contain a header row and must have three columns. A sample ImportGroups.csv file is available on the Import Groups page. The following table describes the required values in the CSV file for importing groups:

Column	Header Value	Value
A	EXTERNAL_ID	External group ID — A unique value that identifies the group. This ID should be persistent and unchanging for the life of the group. The ID is assigned by your organization. It is recommended that you determine a group ID strategy that best suits your needs. If you are manually synchronizing the groups in your Evidence.com agency with groups in another application, you may want to use an ID value provided by the other application, such as a GUID. To find the external group ID for an existing group, view the Group Profile page for the group. You can also simply assign a descriptive name. Valid external group IDs can be up to 255 characters.
B	NAME	Group title — A meaningful name for the group. Because EXTERNAL_ID value provides the persistent identifier for the group, you can change the NAME value as needed. Valid group titles can be up to 255 characters.
C	VISIBLE_TO_FEDERATED	Whether partner agencies are allowed to share cases with the group. Valid values are the following two words: • TRUE • FALSE The valid values are case insensitive.

For more information about valid CSV formatting, see https://tools.ietf.org/html/rfc4180

1. If you have already prepared your groups CSV file, skip to step 9.
2. On the menu bar, click **Admin** and then, under **Users**, click **Import Groups**.

3. Under **Import Groups**, click **ImportGroups.csv** and save it to your computer.



IMPORT GROUPS

This option will build the framework of groups for your agency as specified by the .csv file you upload. This will not assign users to be members of any of the groups that get created. Accepted file type is comma separated value (.csv).

Need an example?

ImportGroups.csv [?]

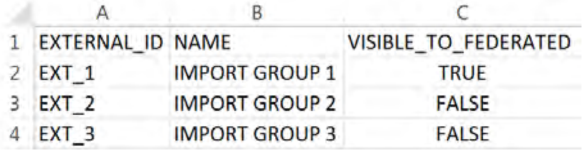
☑ DO NOT MAKE CHANGES TO ANY GROUPS THAT CURRENTLY EXIST.

GROUPS FILE: No file chosen

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	VISIBLE_TO_FEDERATED
2	EXT_1	IMPORT GROUP 1	TRUE
3	EXT_2	IMPORT GROUP 2	FALSE
4	EXT_3	IMPORT GROUP 3	FALSE

6. Delete the second, third, and fourth rows. *Do not* delete the first row. Evidence.com expects the first row to contain the column names.

7. For every group that you want to add, include a row in the file that specifies values for the group, as described in the preceding table. Ensure that each value is in the cell beneath the applicable header.

8. Save your groups CSV file.

9. In Evidence.com, if your session has timed out, sign in again and return to the Import Groups page by clicking **Admin** and then, under **Users**, clicking **Import Groups**.

10. If you want to *completely replace all groups currently in your agency* with the groups in your groups CSV file, click to clear the **Do Not Make Changes To Any Groups That Currently Exist** check box.

    Note: It is recommended that you use the Do Not Make Changes To Any Groups That Currently Exist check box with caution. If you clear the check box and import a CSV file, only the groups in the CSV file exist after the import. Any other groups that previously existed in your agency are deleted.

11. If you want to add the groups in the CSV file without affecting any existing groups, select the **Do Not Make Changes To Any Groups That Currently Exist** check box.

    By default, the Do Not Make Changes To Any Groups That Currently Exist check box is selected.

12. Next to **Groups File**, click **Choose File** and, in the dialog box that opens, select the groups CSV file on your computer, and then click **Next**.

    Evidence.com displays a list actions taken based on the groups found in the uploaded file. This includes information about errors that Evidence.com detected and about the deletion of previously existing groups that were not defined in the groups CSV file.

13. Review the list of actions taken.

14. If you need to correct errors, update the groups CSV file as needed, click **Import More Groups, Members, and Monitors**, and repeat this procedure.

15. Click **Finished**.

    The All Groups page appears.

Define Members and Monitors

You can import definitions for group members and monitors. You define the members and monitors in a CSV file.

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.

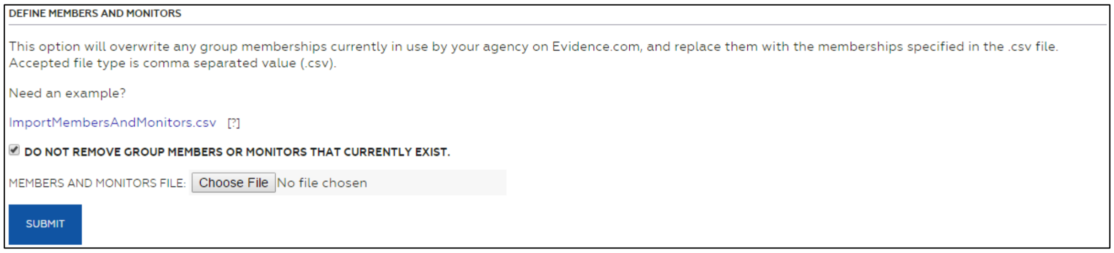
Note: Only the groups referenced in column A of the members-and-monitors CSV file are affected when you define members and monitors. For example, if groups 1 and 2 each have several members assigned and then you import a members-and-monitors CSV file that only includes rows that define members and monitors 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	External group ID — The ID of the group to which the member or monitor is added. This ID must match the external group ID used to create the group. For more information, see Import Groups. If you specify an external group ID that does not correspond to an existing group in your agency, Evidence.com does not create the member or monitor and an error message appears in the list of actions taken. Valid external group IDs can be up to 255 characters.
B	MEMBERSHIP_TYPE	Member or monitor — Whether the row in the CSV file defines a member or a monitor. Valid values are the following two words: • MEMBER • MONITOR The valid values are case insensitive.
C	ENTITY_TYPE	User or group — Whether the member or monitor is a user or a group. Valid values are the following two words: • USER • GROUP The valid values are case insensitive.
D	ENTITY_ID	Identifier of the member or monitor. • If the member or monitor is a group, this value is the external group ID, which must match the external group ID used to create the group. • If the member or monitor is a user, this value must be the email address configured in the user account in your Evidence.com agency.

For more information about valid CSV formatting, see https://tools.ietf.org/html/rfc4180

1. If you have already prepared your members-and-monitors CSV file, skip to step 9.
2. On the menu bar, click **Admin** and then, under **Users**, click **Import Groups**.
3. Under **Define Members and Monitors**, click **ImportMembersAndMonitors.csv** and save it to your computer.



DEFINE MEMBERS AND MONITORS

This option will overwrite any group memberships currently in use by your agency on Evidence.com, and replace them with the memberships specified in the .csv file. Accepted file type is comma separated value (.csv).

Need an example?

ImportMembersAndMonitors.csv [?]

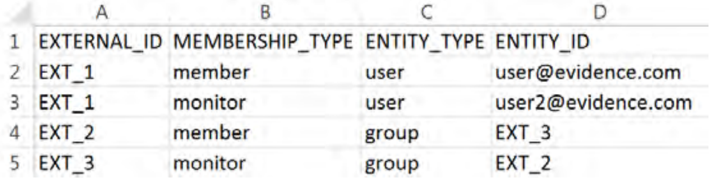
☑ DO NOT REMOVE GROUP MEMBERS OR MONITORS THAT CURRENTLY EXIST.

MEMBERS AND MONITORS FILE: Choose File No file chosen

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. In Evidence.com, if your session has timed out, sign in again and return to the Import Groups page by clicking **Admin** and then, under **Users**, clicking **Import Groups**.

10. If you want to *completely replace all members and monitors* in the groups referenced in column A of the members-and-monitors CSV file, click to clear the **Do Not Remove Group Members Or Monitors That Currently Exist** check box.

    Note: It is recommended that you use the Do Not Remove Group Members Or Monitors That Currently Exist check box with caution. If you clear the check box and import a CSV file, then in the groups referenced in column A of the CSV file, only the members and monitors defined in the CSV file exist after the import. Any other members and monitors that previously existed those groups are removed. Groups not referenced in column A of the CSV file are unaffected.

11. If you want to add the members and monitors in the CSV file without affecting any existing members and monitors, select the **Do Not Remove Group Members Or Monitors That Currently Exist** check box.

By default, the Do Not Remove Group Members Or Monitors That Currently Exist check box is selected.

12. Next to **Members and Monitors File**, click **Choose File** and, in the dialog box that opens, select the CSV file on your computer, and then click **Next**.

    Evidence.com displays a list actions taken based on the members and monitors found in the uploaded file. This includes information about errors that Evidence.com detected.

13. Review the list of actions taken.

14. If you need to correct errors, update the CSV file as needed, click **Import More Groups, Members, and Monitors**, and repeat this procedure.

15. Click **Finished**.

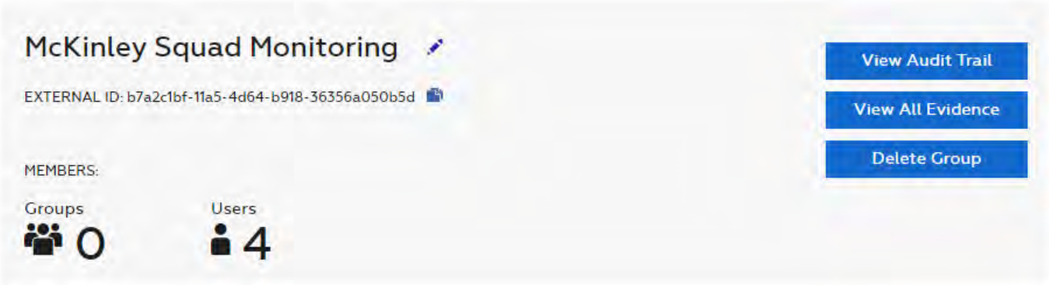
    The All Groups page appears.

Search and View Groups

As with the management of evidence, cases, devices, and users, Evidence.com provides a search feature to help you find groups that you need to work with.

For each group in search results, you can access a Group Profile page, which shows the group title and number of members. The external ID appears below the group title. For groups created by the Create Group page in Evidence.com, the external ID is a hyphenated hexadecimal number automatically assigned by Evidence.com. For groups created by an external source, such as imported CSV file, the Evidence.com Partner API, or automatic provisioning with Microsoft Azure Active Directory, the external ID is the value assigned by external source.

The page also provides access to the group monitor list, the group audit trail, a list of all evidence owned by members of the group, and whether the group can receive evidence shared by a partner agency.



McKinley Squad Monitoring

EXTERNAL ID: b7a2c1bf-11a5-4d64-b918-36356a050b5d

MEMBERS:

Groups 0

Users 4

Users with permission to perform user searches can access the Group Search feature on the Users menu.

1. On the menu bar, click **Admin** and then under **Users**, click **All Groups**.

   The All Groups page shows the search filters and the default search results.

2. If you want more specific results, set the group search options and click **Search**.

   Note: The Member and Monitor search options support filtering by users only. You cannot filter by groups who are members or monitors.

   The search results appear below the search form. Deleted groups appear in search results so that you can access their audit trails.

3. If you want to sort the results, click the column that you want to sort by. You can sort by group title, status, date last modified, and whether groups can receive cases shared by partner agencies.

4. If you want to improve the search results, update the search options as needed, and click **Search** again.

5. If you want to view details about a group, click the group title.

   The Group Profile page appears.

Dashboard List for Monitors

If a user is a monitor of one or more groups, the Groups I Monitor section appears on the user's Dashboard. This area lists the groups in which the user is a monitor. For each group in the list is link to the applicable Group Profile page. For more information, see Dashboard.

My Profile Page for Members and Monitors

A user's account profile page may include group-related lists.

- Groups I Monitor — Appears if the user has evidence-monitoring permission for a group.

- Groups I Am Member Of — Appears if the user is a member of any group.

The user can access the profile page for a group by clicking the group title.

For more information about the user account page, see Update Your Basic Account Information.

User Accounts of Members and Monitors

Administrators and others who are allowed the User Administration permission can see a “Groups I Monitor” list on the profile page of any user who has evidence-monitoring permission for a group. For more information about accessing a user profile page, see Edit Other User Account Information.

Edit Group Members, Monitors, and Other Settings

Users with permission to edit a group can make changes to all settings associated with a group.

1. In your Evidence.com agency, search for the group for which you need to make changes.
2. In the group search results, click the group title.

   The profile page for the group that you clicked appears.

3. Edit the group as needed. For detailed steps, refer to the following table.

Task	Steps
Change the group title	1. To the right of the group title, click ✎ (edit). 2. Type the new title. 3. Click **Save**.
Add a user or group to any of the following: • Members • Monitors of this group • Who this group can monitor	1. As needed, click to expand the panel you need to open – **Members** or **Monitors**. 2. Click in the box that you need: **Add Member**, **Monitors of this Group**, or **This Group Can Monitor**. 3. Start typing the name of the user. 4. Wait for Evidence.com to show the list of matching users. 5. Click the user you want to add. 6. Click **Add**.
Delete a user or group from any of the following lists: • Members • Monitors of this group • Who this group can monitor	1. As needed, click to expand the panel you need to open – **Members** or **Monitors**. 2. In the list that you need to edit, find the user or group. 3. To the left of the user or group name, under **Actions**, click ✕.
Change whether the group can receive evidence shared by a partner agency	1. As needed, click to expand **Monitors** panel. 2. Select or click to clear the **Allow Partner Agencies to share with this group** check box.
Copy the external ID of the group	The external ID appears below the group title. To copy it, click the icon to the right of the external ID.

View All Evidence

Users who have evidence-monitoring permission for a group can view a list of all the evidence uploaded by group members or shared with the group by a partner agency. Administrators can also view all evidence owned by group members.

1. In your Evidence.com agency, search for the group for which you need to view evidence. For more information, see Search and View Groups.
2. In the group search results, click the group title.

   The Group Profile page appears.
3. Click **View All Evidence**.

   The All Evidence page lists all evidence uploaded by members of the group or shared with the group by a partner agency.
4. If you want to view evidence, click the evidence title.

   Evidence.com displays detailed information about the evidence.
5. If you want access to another member's evidence, click Request Access for the evidence.

   Evidence.com sends you a notification email when the member has granted you access to the evidence.

View Group Audit Trail

Users who have permission to view group audit trails can do so from the Group Profile page of any group. For deleted groups, viewing the audit trail is the only available action.

To perform this task, you must be allowed the Group Audit Trail PDF permission.

1. In your Evidence.com agency, search for the group for which you need to view the audit trail. For more information, see Search and View Groups.
2. In the group search results, click the group title.

   The Group Profile page appears.
3. Click **View Audit Trail**.

   A dialog box provides options for viewing the entire audit trail or a portion of the audit trail.

4. If you want to view the whole audit trail, under **View entire audit log**, click **Submit**.
5. If you want to view a portion of the audit trail, under **View portion of audit log**, specify a date in either or both the **From** or **To** boxes and click **Submit**.

   Evidence.com opens or downloads a PDF for the agency audit trail. The exact behavior depends on the browser you use and its download settings for PDF files.
6. Save or view the audit trail PDF as needed.

Delete Group

Users who have permission to edit groups can change the status of an active group to Deleted. When you delete a group, the access of monitors to evidence uploaded by members of the group is revoked.

Note: Deleted groups cannot be re-activated.

The audit trail for a deleted group remains available for users who have permission to view group audit trails.

Delete Group from Group Search Results

1. In your Evidence.com agency, search for the group you want to delete.
2. In the group search results, to the left of the group title, click ✕ (delete group).
3. On the confirmation message box, click **OK**.

   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 **Edit Group**.

The Edit Group Profile page appears.

4. Click **Delete Group**.

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

   Evidence.com changes the state of the group to Deleted.

   The Edit Group Profile page updates and the only action available is View Audit Trail.

Roles and Permissions

Roles determine user permissions, which control access to features and functions. Each Evidence.com user is assigned a role.

Administrators and users whose role allows the Edit Agency Settings permission can create roles and edit roles.

Administrators and users whose role allows the User Administration permission can assign roles to users.

By default, Evidence.com provides all agencies with locked roles or pre-configured roles. Locked roles cannot be changed by your agency.

The preconfigured and locked roles are different for Evidence.com PRO and LITE agencies.

PRO Agency Pre-Configured Role	Locked or Configurable
Admin	Locked
User	Configurable
Investigator	Configurable
Armorer	Configurable
Assignee Only	Locked

For more information, see PRO Agency Pre-Configured Roles and Default Permissions.

LITE Agency Pre-Configured Role	Locked or Configurable
Lite Admin	Locked
Lite User	Locked
Lite Armorer	Locked
Assignee Only	Locked

For more information, see LITE Agency Pre-Configured Roles and Default Permissions.

About the Assignee Only Role

Users assigned to the Assignee Only role do not have access to your Evidence.com agency. Devices can be assigned to these users. This role allows an agency administrator to assign devices to several officers without requiring them to register for an Evidence.com account.

All permissions for the Assignee Only role are set to Prohibited. When these users are added, the Evidence.com system generates a random password and their status is immediately shown as Active within your agency's Evidence.com account but they do not receive any email notifications. When users assigned to this role try to reset their password, an error message is displayed.

Note: Evidence recorded on devices assigned to users whose role is Assignee Only can be uploaded to Evidence.com by your agency's administrator or by any user whose role allows the required permissions.

About the Restricted Category Access Permission

If an evidence file contains highly sensitive information, administrators can implement the Restricted Category Access feature. If you assign evidence to a restricted category, only users whose role allows the Restricted Category Access permission can see the evidence. For example, your agency may want to create an Internal Affairs role that allows access to evidence assigned to a restricted category.

In addition, a role allowed the Restricted Category Access permission should also have the Evidence View permission set to Any Evidence.

Dependencies Among Permissions

Some permissions cannot be allowed unless you have allowed a permission that they are based upon. For example, the Evidence Edit permission is not available unless you allow the Evidence View permission. Likewise, the Evidence Redact permission is not available unless you allow the Evidence Edit permission.

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.

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.

   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 roles 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 **Add New 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. 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.

5. 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 name of 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. 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 name of the permission.

5. 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.

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

   In the search results, the newly applied user roles appear.

Agency Profile

The agency profile enables you to specify details about your agency, such as street address, logo, and description. Through the Agency Profile page, you can access the agency audit trail.

Configure Agency Street Address

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Agency Profile**.

   The Agency Profile page appears.
2. Click **Edit Address**.
3. In the boxes and lists provided, specify the agency street address.
4. When you have finished editing the address, click **Submit**.

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

   The Agency Profile page displays the new street address.

Configure Agency Logo

The agency logo appears on audit trail PDFs and system-generated emails.

You can upload a logo file from a location available to the computer you are using to access Evidence.com.

Logo file size must be less than five MB.

The logo file type must be GIF, JPG, JPEG, BMP, TIF, or PNG.

You also have the option of deleting the logo.

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Agency Profile**.

   The Agency Profile page appears.

2. Click **Change Logo**.

3. If you want to specify a new logo, click **Choose File**, select the logo file, and click **Save**.

   The file uploads to Evidence.com.

4. If you want to remove the logo, click **Delete Logo**.

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

   The Agency Profile page shows the logo that you uploaded or, if you deleted the logo, shows a placeholder Evidence.com logo.

Configure Agency Description

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Agency Profile**.

   The Agency Profile page appears.

2. Click **Edit Description**.

3. In the box provided, type the agency description.

4. When you finish updating the description, click **Save Changes**.

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

   The Agency Profile page displays the description that you provided.

View Agency Audit Trail

The Agency Audit Trail shows agency-wide changes to your Evidence.com account. This report helps provide transparency on administrative actions across Evidence.com. By displaying each action in detail, your agency is able to review who changed a setting, in order to understand the purpose and provide better accountability to each user.

The audit trail logs the following Evidence.com changes:

- Device Default Ownership Policy Updated
- Address Added
- Address Updated
- Admin Added
- Admin Changed
- Authentication Policy Updated
- Partner Created
- Default Retention Level Updated
- Axon Body Settings Updated
- Flex Settings Updated
- Axon ATC Settings Updated
- Device Settings Updated
- X2 Settings Updated
- Dual Factor Authentication Policy Updated
- Expire All Subscriber Passwords of Partner Agency
- Partner Federation Entity Removed
- Partner Federation Entity Updated

- Federation Group Updated
- Partner Federation Updated
- Partner Federation Disabled
- IP Address Policy Updated
- IP Range Restriction Updated
- IP Address Session Security Policy Updated
- Password Policy Updated
- Agency Deactivated
- Agency Reactivated

Any user with the Edit Agency Settings permission Allowed under ADMIN ACCESS can view the Agency Audit Trail

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Agency Profile**.

   The Agency Profile page appears.

2. Click **View Audit Trail**.

   A dialog box provides options for viewing the entire audit trail or a portion of the audit trail.

3. If you want to view the whole audit trail, under **View entire audit log**, click **Submit**.

4. If you want to view a portion of the audit trail, under **View portion of audit log**, specify a date in either or both the **From** or **To** boxes, and then click **Submit**.

   Evidence.com opens or downloads a PDF for the agency audit trail. The exact behavior depends on the browser you use and its download settings for PDF files.

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

Evidence ID Validation

You can use the evidence ID validation feature to help ensure that Evidence.com users enter evidence IDs correctly. If all evidence associated with a case has the same ID as the case, Evidence.com makes it easy to add evidence to cases. Errors in evidence IDs can lead to confusion and lost time while users search for misidentified evidence, fix the ID, and add it to the associated case. Evidence ID validation can help prevent errors when users add or update evidence IDs, leading to greater operational efficiency.

By default, Evidence.com does not validate evidence IDs.

Note: Evidence ID validation applies to data entered by users on your Evidence.com agency web site only. Evidence ID validation does not affect data uploaded by Evidence Sync for Microsoft Windows, Axon Capture for iOS and Android, or Axon View for iOS and Android.

Regular Expressions for Evidence ID Validation

Using standard Javascript regular expression notation, you can describe your agency's evidence ID format requirements. In order for an evidence ID to be valid, the ID 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 ID validation to be case *sensitive*, the regular expression must end with the following two characters: `$/`
- If you need ID validation to be case *insensitive*, the regular expression must end with the following three characters: `$/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 study Javascript regular expressions prior to implementing evidence ID validation in your Evidence.com agency.

TASER Professional Services is available to assist you with developing a regular expression that fits the needs of your agency. For more information, contact your local TASER representative.

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/

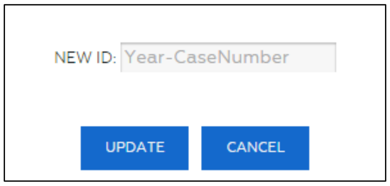
Example Regular Expressions

The following table provides a few examples of ID formats and regular expressions that match only IDs that comply with the ID format.

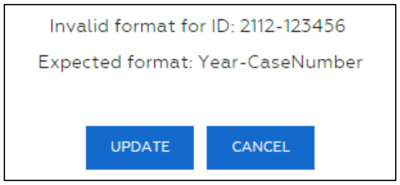
ID Format Example & Description	Matching Regular Expressions and Comments
YYYYMMDDnnnnnn Four-digit year, two-digit month, two-digit day, and 6-digit number.	The following regular expression matches the YYYYMMDDnnnnnn format and requires that the ID begin with 20; however, it does not account for months 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 IDs, users see *hint text* that reflects the ID format requirements. For example, a user changing evidence IDs on an evidence search page sees the following dialog box:



If a user enters an evidence ID that does not match the regular expression configured for ID validation, Evidence.com does not allow the user to assign the ID to the evidence. In the error message that appears, Evidence.com indicates that the ID is not valid and provides the hint text again.



Invalid format for ID: 2112-123456

Expected format: Year-CaseNumber

Configure Evidence ID Validation

Administrators and users who are allowed both the Category Administration and the Edit Agency Settings permissions can configure evidence ID validation.

Whether you are enabling evidence ID validation for the first time or updating the regular expression, the steps for configuring evidence ID validation are the same.

1. On the menu bar, click **Admin** and then click **Fields & Retention Categories**.
2. In the **Regex** box, enter the regular expression that you want to use to validate evidence IDs.
3. In the **Descriptor** box, enter the text that you want to appear as hint text in evidence ID fields.
4. 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 **Fields & Retention Categories**.
2. Under **Field Validation**, click **Disable**.

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, restricted access for especially sensitive evidence, and the appearance of evidence map pins.

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.

  You cannot change the evidence retention policy for this category. Evidence assigned to this category must be manually deleted.

- Pending Review — You cannot make the Pending Review category a restricted category.

You cannot delete the Uncategorized or Pending Review category.

When TASER created your agency, we provided four additional categories that you can edit and delete as needed:

- Officer Injury
- Traffic Stop
- Training Demo
- Use of Force

Evidence Retention Policy

The evidence retention policy determines:

1. Whether Evidence.com initiates automatic deletion of evidence assigned to the category.
2. How long Evidence.com waits before initiating the deletion of evidence that is not included in a case. All evidence deletions are based on the recording date.

To protect against accidental deletions, administrators can recover files up to 7 days after they are queued for deletion.

This policy applies to evidence only. Cases are never deleted automatically.

Evidence included in a case is exempt from deletion until it is removed from the case.

If evidence is in multiple categories, the longest retention time is used.

Evidence.com sends the following notification emails about evidence queued for deletion:

- Administrators receive a weekly email that summarizes upcoming agency-wide deletions.
- Users receive a weekly message regarding evidence that they uploaded.

For administrators, the Dashboard includes an Upcoming Evidence Deletions section that lists both user-initiated and system-initiated deletions.

Restricted Categories

The Categories feature provides the ability to restrict access to evidence that is especially sensitive. In order to see evidence that you assign to a restricted category, users must be assigned a role that is allowed the Restricted Category Access permission.

By default, all new and pre-configured categories are not restricted categories.

By default, all new roles and all pre-configured roles are not allowed the Restricted Category Access permission.

Map Pin Style

Categories determine the appearance of the pins shown on evidence maps. You can specify the shape and color of map pins.

Add a Category

You can create categories as needed. A new category has the following default settings:

- Map Pin Style — Blue circle
- Evidence Retention — Until manually deleted
- Restricted Category — Not restricted

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Fields & Retention Categories**.

   The Fields & Retention Categories page appears.

2. Click **New Category**.

   The New Evidence Category page appears.

3. Under **Category Name**, type a **Name** for the new category.

4. If you want to change the pin style, in the lists under **Map Pin Style**, click the color and shape that you want.

5. Specify the retention duration for evidence in this category.

   - If you want Evidence.com to initiate deletion of evidence after a retention period, in the **Keep evidence** list, click a unit of time and then, in the box, type the length of the retention period.

   - If you do not want Evidence.com to initiate the deletion of evidence in this category, in the **Keep evidence** list, click **Until manually deleted**.

6. Under **Restricted Category**, specify whether the category is a restricted category.

   - If you *do not* want to require that users must be allowed the Restricted Category Access permission in order to see evidence in this category, in the list click **No Restrictions**.

   - If you want to require that users must be allowed the Restricted Category Access permission in order to see evidence in this category, in the list click **Restricted Category**.

7. Click **Save Category**.

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

   The Fields & Retention Categories page lists the category you added.

Edit a Category

It is recommended that, *before* you edit a category, 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 **Fields & Retention Categories**.

   The Fields & Retention Categories page appears.

2. For the category that you want to edit, under **Options**, click **Edit**.

   The Edit Category appears.

3. Edit the category as needed. For detailed steps, refer to the following table.

Task	Steps
Change the category name	Under **Category Name**, type the new name.
Change the pin style	In the lists under **Map Pin Style**, click the color and shape that you want
Set a retention period for evidence assigned to this category	1. In the **Keep evidence** list, click a unit of time. 2. In the box, type the length of the retention period.
Ensure that evidence in this category is retained indefinitely	In the **Keep evidence** list, click **Until manually deleted**.
Restrict access to evidence assigned to the category	In the list under **Restricted Category**, click **Restricted Category**.
Remove restrictions from access to evidence assigned to the category	In the list under **Restricted Category**, click **No Restrictions**.

4. When you have finished editing the category, click **Save Category**.

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

   Evidence.com saves the changes you made to the category and begins enforcing the effects of the changes.

Delete a Category

It is recommended that, *before* you delete a category, 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 **Fields & Retention Categories**.

   The Fields & Retention Categories page appears.

2. For the category that you want to delete, under **Options**, click **Delete**.

   A dialog box lists the number of evidence files that are currently in the category you are deleting.

3. In the **Transfer all evidence categorized as *Category*** to list, click the list that you want to assign to the evidence files.

4. Click **Delete Category**.

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

   The Fields & Retention Categories page no longer lists the category you deleted.

Device Settings

Under Device Settings on the Admin portal page, administrators can access settings for the following features:

- Camera Settings
- CEW Settings

Configure Camera Settings

The Camera Settings page enables agency administrators to define settings for Axon devices, such as Axon Body 2, Axon Body, and Axon Flex. The page provides settings such as video quality, event pre-buffering, audio mute control, and indicator light control.

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

Microphone controls are intended for agencies in locations with restrictions on audio recordings.

Video quality settings provide the ability to define the Axon video encoding rate or the space used per hour of recording. This is useful for agencies wanting to reduce the impact of Axon video uploads on the agency's Internet connection.

Note: To ensure that the quality of videos is acceptable, it is strongly recommended that you always validate the effect of the configured camera settings.

1. On the menu bar, click **Admin**, and then under **Device Settings**, click **Camera Settings**.

   The Camera Settings page displays sections for Axon Flex and Axon Body settings, Axon Body 2 settings, and settings affecting all Axon cameras.

2. For each setting, choose the option that best supports your agency's policies regarding video, audio, and offline camera usage.

3. At the bottom of the page, click **Save Settings**.

   Evidence.com saves the camera settings. Axon Dock and Evidence Sync updates each camera with any changed settings the next time that the camera is connected.

Configure CEW Settings

The CEW Settings page enables administrators to configure Conducted Electrical Weapons (CEW) Settings based on agency policy.

Before you perform the following steps, ensure that you have installed Evidence Sync. For more information, see Download and Install Evidence Sync.

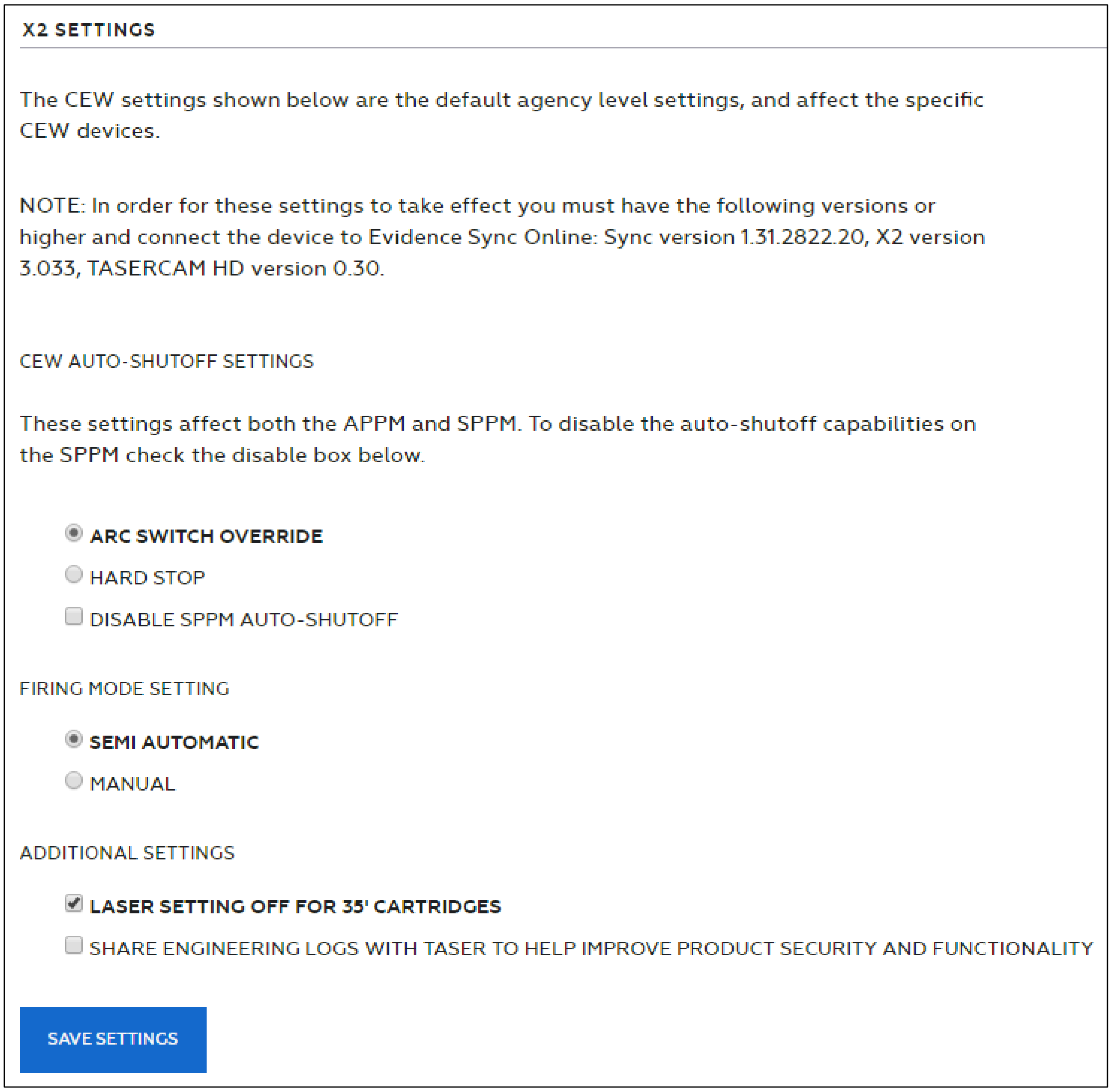
1. On the menu bar, click **Admin** and then under **Device Settings**, click **CEW Settings**.

   The CEW Settings page appears.

2. Configure the **CEW Auto-Shutoff** Settings and **Firing Mode** Settings and the optional **Additional** Settings.

   In the figure below, the ARC Switch Override, Semi Automatic, and “Laser setting off for the 35” cartridges” options are selected.

   Note: These settings are automatically applied to all the X2 devices assigned to your agency whenever those devices are next connected using the Evidence Sync application.



X2 SETTINGS

The CEW settings shown below are the default agency level settings, and affect the specific CEW devices.

NOTE: In order for these settings to take effect you must have the following versions or higher and connect the device to Evidence Sync Online: Sync version 1.31.2822.20, X2 version 3.033, TASERCAM HD version 0.30.

CEW AUTO-SHUTOFF SETTINGS

These settings affect both the APPM and SPPM. To disable the auto-shutoff capabilities on the SPPM check the disable box below.

● **ARC SWITCH OVERRIDE**

○ HARD STOP

□ DISABLE SPPM AUTO-SHUTOFF

FIRING MODE SETTING

● **SEMI AUTOMATIC**

○ MANUAL

ADDITIONAL SETTINGS

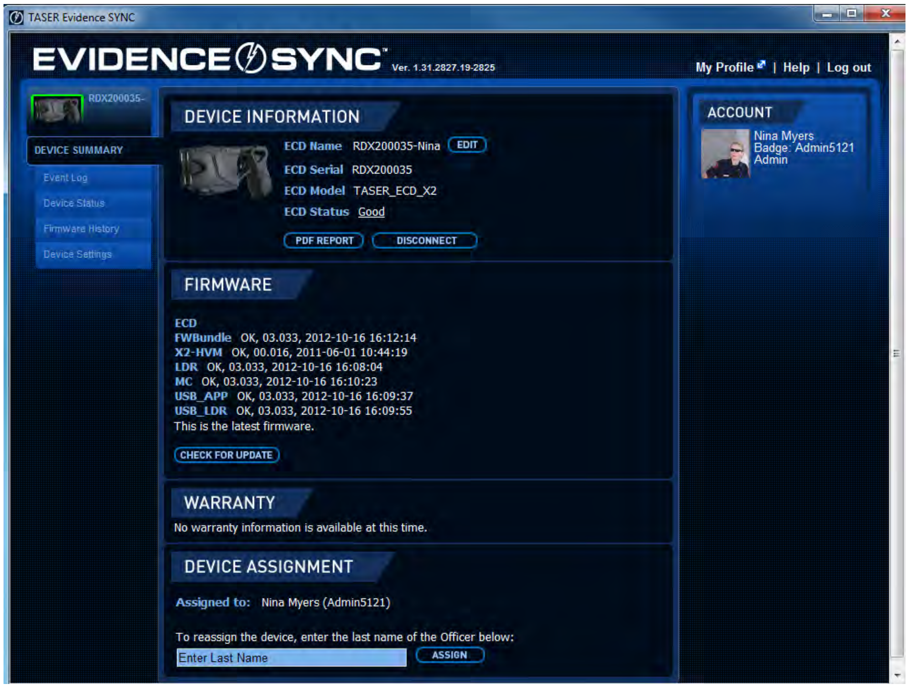
☑ **LASER SETTING OFF FOR 35' CARTRIDGES**

□ SHARE ENGINEERING LOGS WITH TASER TO HELP IMPROVE PRODUCT SECURITY AND FUNCTIONALITY

3. Click **Save Settings**.

4. Launch the **Evidence Sync** (version 1.31.2836.20-2837 or higher) application. Connect an X2 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.



TASER Evidence SYNC

EVIDENCE SYNC Ver. 1.31.2827.19-2825

My Profile | Help | Log out

RDX200035-

DEVICE SUMMARY
Event Log
Device Status
Firmware History
Device Settings

DEVICE INFORMATION

ECD Name RDX200035-Nina EDIT
ECD Serial RDX200035
ECD Model TASER_ECD_X2
ECD Status Good

PDF REPORT DISCONNECT

FIRMWARE

ECD
FWBundle OK, 03.033, 2012-10-16 16:12:14
X2-HVM OK, 00.016, 2011-06-01 10:44:19
LDR OK, 03.033, 2012-10-16 16:08:04
MC OK, 03.033, 2012-10-16 16:10:23
USB_APP OK, 03.033, 2012-10-16 16:09:37
USB_LDR OK, 03.033, 2012-10-16 16:09:55
This is the latest firmware.

CHECK FOR UPDATE

WARRANTY

No warranty information is available at this time.

DEVICE ASSIGNMENT

Assigned to: Nina Myers (Admin5121)

To reassign the device, enter the last name of the Officer below:

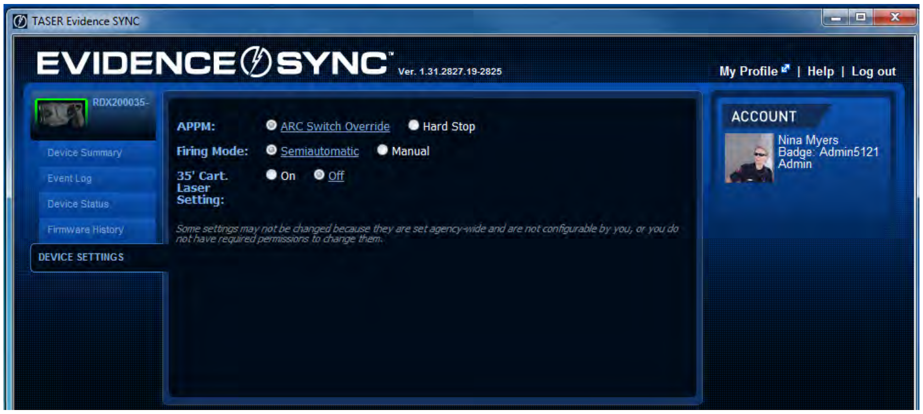
Enter Last Name ASSIGN

ACCOUNT

Nina Myers
Badge: Admin5121
Admin

5. Click the **Device Settings** tab.

The CEW Settings options that were selected in your agency's Evidence.com account appear.



TASER Evidence SYNC

EVIDENCE SYNC Ver. 1.31.2827.19-2825

My Profile | Help | Log out

RDX200035-

Device Summary
Event Log
Device Status
Firmware History
DEVICE SETTINGS

APPM: ● ARC Switch Override ○ Hard Stop
Firing Mode: ● Semiautomatic ○ Manual
35' Cart. Laser Setting: ○ On ● Off

Some settings may not be changed because they are set agency-wide and are not configurable by you, or you do not have required permissions to change them.

ACCOUNT

Nina Myers
Badge: Admin5121
Admin

Note: These settings cannot be configured in Evidence Sync. To change any of these X2 device settings, you must sign in to your agency's Evidence.com administrator account and change them from the Settings > Configuration Settings > CEW Settings option.

Security Settings

Under Security Settings on the Admin portal page, administrators can access settings related to site security.

IP Security

By enabling the IP Security, agency administrators can define who is allowed or not allowed to access their agency's Evidence.com accounts based on the IP address. By default, when TASER creates your Evidence.com agency, IP security is disabled and your agency's sign-in page can be accessed from anywhere within your country.

If you enable IP security, you can authorize specific IP addresses and ranges of IP addresses, such as the IP addresses used at your agency headquarters or at specific districts. Only devices assigned one of the authorized IP addresses can access your Evidence.com agency.

Note: Before you enable IP security, work with your IT staff and your Internet provider to acquire static (non-changing) IP addresses. If you do not use static IP addresses, your agency could be denied access from its own Evidence.com agency. Consumer-grade Internet lines, such as DSL or cable modems, typically have a 200-hour lease. This means that every 200 hours the IP address is refreshed with a new one.

1. On the menu bar, click **Admin** and then under **Security Settings**, click **IP Address**.

   The IP Active Session Security area appears at the top of the page.

2. To enable IP Address Security, in the **IP Address** field, enter the known IP address or default gateway that is seen by the Internet for your agency. You must enter a Starting and Ending IP Address if you select **Range of IP Address**.

3. Enter a useful description of this address in the **Label** field. The Label field is optional but descriptive labels help make managing your Evidence.com account easier.

4. Click **Add Allowed IP Address** to add the location.

5. Click the **Enable IP Security** checkbox located at the top of the page.

   The newly added IP Address shows in the table.

6. You can continue adding additional IP Addresses as required.

7. If at any time you want to prevent access from any IP addresses, click the corresponding **Delete** link. However, to prevent being locked out of your account ensure that you do *not* delete your current IP address.

IP Whitelisting for Multi-Homed Networks

Evidence.com supports IP security whitelists for agencies where web traffic can originate from multiple IPs during the same user session. The standard IP whitelist security detects if an active user changes source IP address in the middle of a session and logs the user out. The new setting still restricts site usage to the IP whitelist ranges, but does not terminate a user session if there is an IP change mid-session.

This setting is designed for agencies using network designs where web traffic is sourced from multiple IPs. For example, networks with multiple firewalls or proxy servers can exhibit this behavior. Agencies that load balance outbound traffic across multiple network links also fall into this category. These designs are perfectly valid but cause a false positive for our “Man in the Middle” protection. Until now, these agencies have not been able to utilize our IP whitelist security.

If your agency is not using this type of design, it is recommended that you employ the standard IP session security for the highest levels of protection.

1. On the menu bar, click **Admin** and then under **Security Settings**, click **IP Security**.
2. Enter in a single IP address or a range of addresses to trust.
3. Check the **Allow IP Address To Change During An Active Session To The Trusted IP Addresses Below** check box.

Mobile Phone Advanced Authentication

By enabling Mobile Phone Advanced Authentication, agency administrators can add a layer of security to their Evidence.com agencies.

This requires users to have access to their mobile phone as well as their username and password when they sign in. This means that if someone steals or guesses their password, the potential hijacker still cannot sign in to their account because they do not have their phone.

This authentication is also required for critical actions. For example, you are prompted to answer your security questions when you attempt any of the following actions:

- Deleting evidence
- Assigning evidence to a category with a lower retention policy
- Deleting a case

- Assigning a case to a category with a lower retention policy
- Changing a category retention policy
- Deactivating a user
- Changing a user's role
- Changing a role's permission
- Adding or deleting IP addresses or IP address ranges
- Disabling IP restrictions
- Disabling Dual Factor Authentication
- Enabling or disabling any of the Security Settings
- Creating categories

When you answer the questions, the authentication is not required for the number of minutes specified in the Code Request Frequency field on trying any of the above actions.

1. On the menu bar, click **Admin** and then under **Security Settings**, click **IP Security**.

   The Mobile Phone Advanced Authentication settings appear below the IP Active Session Security setting.

   By default, it is disabled (the **Off** option is selected).

2. Choose the method to deliver the verification codes (either **SMS Text** or **Automated Call Back**).

   Note: Ensure that you have verified and saved your cell phone number on your Account Details page before you select either option.

3. Choose how long the verification codes are saved within Evidence.com by entering a valid number in the **Code Request Frequency** field. After the codes expire, users are prompted to enter new codes.

4. Click **Save** when you are done.

   Your agency’s **Security Settings** are now configured and enabled.

Configure Password Settings

This feature enables administrators to define password settings for all users in the agency.

- **Password History** — Unique new passwords a user must use before an old password can be reused. [default 10, min 1, max 25]
- **Password Aging** — Determines how many days a password can be used before the user is required to change it. [default 90, min 7, max 365]
- **Password Length** — Determines how short passwords can be. [default 8, min 6]
- **Failed Login Limit** — Number of failed login attempts before the account is locked out. [default 5, min 1, max 25]
- **Lockout Duration** — Number of minutes a user is locked out of their account due to failed login attempts. [default 60, min 1, max 720]

1. On the menu bar, click **Admin** and then under **Security Settings**, click **IP Security**.

   The Password Configuration page with the various settings appears. Below each setting are a description and the default and maximum (max) values of the setting.

2. Set the options based on your agency's requirements.

   Note: If you want to start over with customizing the password configuration settings, click **Restore Defaults**.

3. When have finished configuring password settings, click **Save**.
4. On the notification message box, click **OK**.

API Settings

Available to Evidence.com PRO agencies who request access to the Evidence.com Partner API, the API Settings page provides administrators the ability to ensure that only authenticated and authorized clients can use the Partner API feature to programmatically configure your Evidence.com agency. The Partner API supports the use of third-party programmatic clients to perform create, read, update, and delete operations on the resources supported by the API, which include the following object types:

- Users
- Groups
- Cases
- Evidence
- Devices
- Reports

For more information, please send inquiries to earlyaccess@taser.com.

Partner Agency Administration

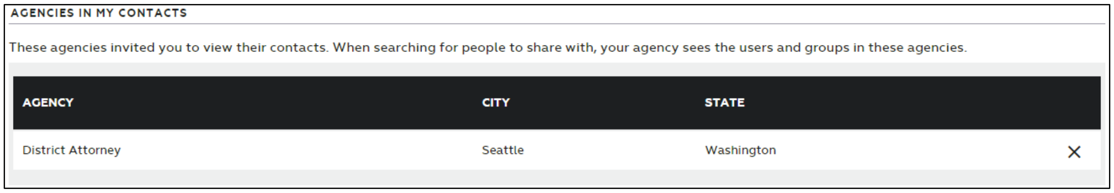
Evidence.com makes it easy for your users to share evidence and cases with other Evidence.com agencies. The agencies you share with or who share with you are *partner agencies*. Partner agencies have access only to data that you specifically share with them. All unshared data owned by your agency remains completely unavailable to partner agencies.

Partner Agency Lists

In the Admin section of your Evidence.com agency, the Partner Agencies page has two lists that administrators can use to control how your agency collaborates with its partner agencies.

- **Agencies In My Contacts** — The agencies whose users and groups are available for your agency to share with. These agencies invited you to view their user and group lists. They have added your agency to their Agencies With My Contacts list.

  When a user in your agency wants to share cases and evidence with a partner agency, the users and groups of these agencies are available and can be found when your user searches for people to share with.



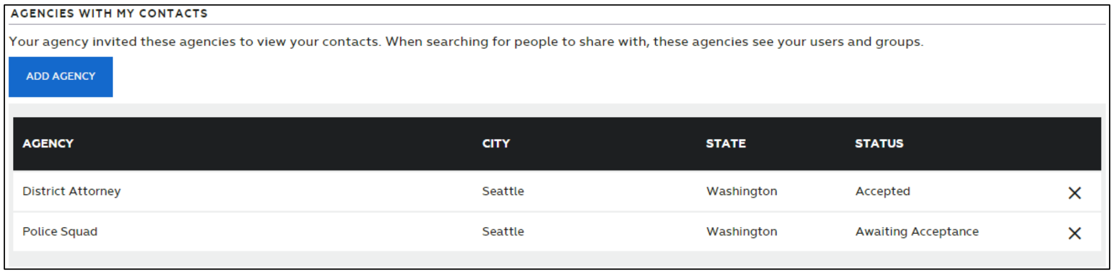
AGENCIES IN MY CONTACTS

These agencies invited you to view their contacts. When searching for people to share with, your agency sees the users and groups in these agencies.

AGENCY	CITY	STATE	
District Attorney	Seattle	Washington	×

- **Agencies With My Contacts** — The agencies that can share with your users and groups. These agencies accepted your invitation to view your directory. They have accepted your invitation and your agency appears on their Agencies In My Contacts list.

  When a user in one of these agencies wants to share cases and evidence with your agency, the users and groups of your agency are available and can be found when the user in the other agency searches for people in your agency to share with.



AGENCIES WITH MY CONTACTS

Your agency invited these agencies to view your contacts. When searching for people to share with, these agencies see your users and groups.

AGENCY	CITY	STATE	STATUS	
District Attorney	Seattle	Washington	Accepted	×
Police Squad	Seattle	Washington	Awaiting Acceptance	×

Sharing with Partner Agencies

Users who are allowed the Share with Partner Agencies permission can share cases with agencies on your Agencies In My Contacts list. Users who are allowed the Share Externally to Authenticated Users permission can share evidence with agencies on your Agencies In My Contacts list.

For more information about sharing with partner agencies, see the following topics:

- Share an Evidence File
- Bulk Share Evidence by Authenticated Sharing
- Share a Case by Download Link
- Share a Case with a Partner Agency

Invite an Agency to Share with Your Agency

In order to allow your users to share cases and evidence with another agency, you must invite the other agency. When you invite an agency, you are sharing your agency's contact list with that agency. Your contact list consists of the following items:

- All your users.
- Your groups that have the "Allow Partner Agencies to share with this group" setting enabled. For more information, see Groups Receiving Shared Cases from Partner Agencies.

Note: Administrators of agencies that you add to your Agencies With My Contacts list receive a notification email. *Before you can share a case with the partner agency*, an administrator from the partner agency must accept the invitation to collaborate with your agency.

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Partner Agencies**.

   The Partner Agencies page appears.

2. Under **Agencies With My Contacts**, click **Add Agency**.

   An agency-search dialog box opens.

3. Search for the agency that you want to allow to share cases and evidence with your agency.

4. In the search results, click the agency name.

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

   The agency appears in the Agencies With My Contacts list, with the status “Awaiting Acceptance”. Administrators of the new partner agency receive an email notifying them of the invitation to receive shared cases and evidence from with your agency.

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

   After the partner agency has accepted the request to collaborate with your agency, users of your agency who have permission to share with partner agencies can share with the new partner agency.

Accepting or Rejecting an Invitation to Collaborate with an Agency

When another agency adds your agency to their Agencies With My Contacts list, Evidence.com sends a notification email to administrators of your agency. Before the other agency can share cases and evidence with your agency, you must accept the invitation.

Alternatively, if you do not want to allow the other agency to collaborate with your agency, you can reject the invitation.

1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Partner Agencies**.

   The Partner Agencies page appears.

2. In the **Agencies In My Contacts** list, find the agency who invited you to collaborate.

3. Do one of the following:

   - If you want to allow your users to share evidence and cases with the other agency, click **Accept**.

     Your agency can now share cases and evidence with the other agency.

     Administrators of the partner agency receive notification emails that you accepted the invitation to collaborate.

   - If you *do not* want to allow your users to share cases and evidence with the other agency, click **Reject** and then, on the confirmation dialog box, click **OK**.

Ending Collaboration with a Partner Agency

If you no longer want to collaborate with a partner agency, remove that agency from the applicable lists on the Partner Agencies page.

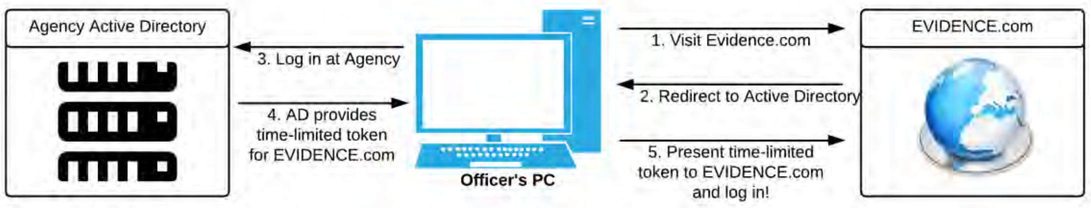
Task	Steps
Prevent a partner agency from sharing cases and evidence with your users.	1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Partner Agencies**. 2. In the **Agencies With My Contacts** list, find the agency and click the corresponding ✕ button. 3. On the confirmation message box, click **OK**. 4. On the notification message box, click **OK**. Your agency can no longer received shared cases and evidence from the other agency.
Prevent your agency from sharing cases and evidence with a partner agency.	1. On the menu bar, click **Admin** and then under **Agency Settings**, click **Partner Agencies**. 2. In the **Agencies In My Contacts** list, find the agency and click the corresponding ✕ button. 3. On the confirmation message box, click **OK**. 4. On the notification message box, click **OK**. Your agency can no longer send shared cases and evidence to the other agency.

Active Directory—Single Sign On

The Active Directory—Single Sign On feature is an Early Access feature and does not appear in your agency account unless you request access. In order to join the program and gain access to this feature, email earlyaccess@taser.com or speak to your local TASER representative.

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.


Agency Active Directory
3. Log in at Agency
4. AD provides time-limited token for EVIDENCE.com
Officer's PC
1. Visit Evidence.com
2. Redirect to Active Directory
5. Present time-limited token to EVIDENCE.com and log in!
EVIDENCE.com

Evidence Management

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

Import Evidence

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

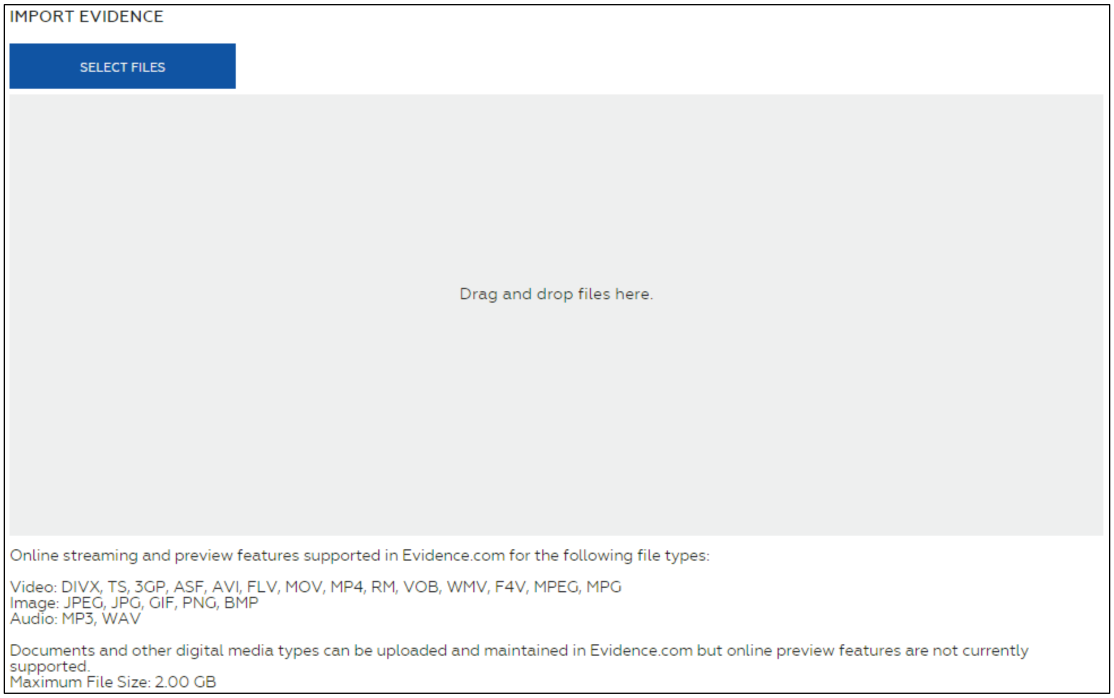
You can use this feature to import evidence that was not recorded on Axon devices, such as pictures taken with your smartphone and saved on your computer.

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

The maximum file size is 2 Gigabytes.

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

   The Import Evidence page appears.



IMPORT EVIDENCE

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
Audio: MP3, WAV

Documents and other digital media types can be uploaded and maintained in Evidence.com but online preview features are not currently supported.
Maximum File Size: 2.00 GB

2. Add the files that you want to import, using either of the following methods:

   - Find the files on your computer and then drag and drop the files onto the Import Evidence page.

   - Click **Select Files** and then use the dialog box to find and select the files on your computer.

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

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 easily add it to the case.
Category	Determines the retention period for evidence that is not assigned to an active case. Uncategorized evidence is retained until it is manually deleted. For sensitive evidence, restricted categories provide additional, permission-based control of who can view the evidence.

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

4. Click **Upload Evidence**.

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

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

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

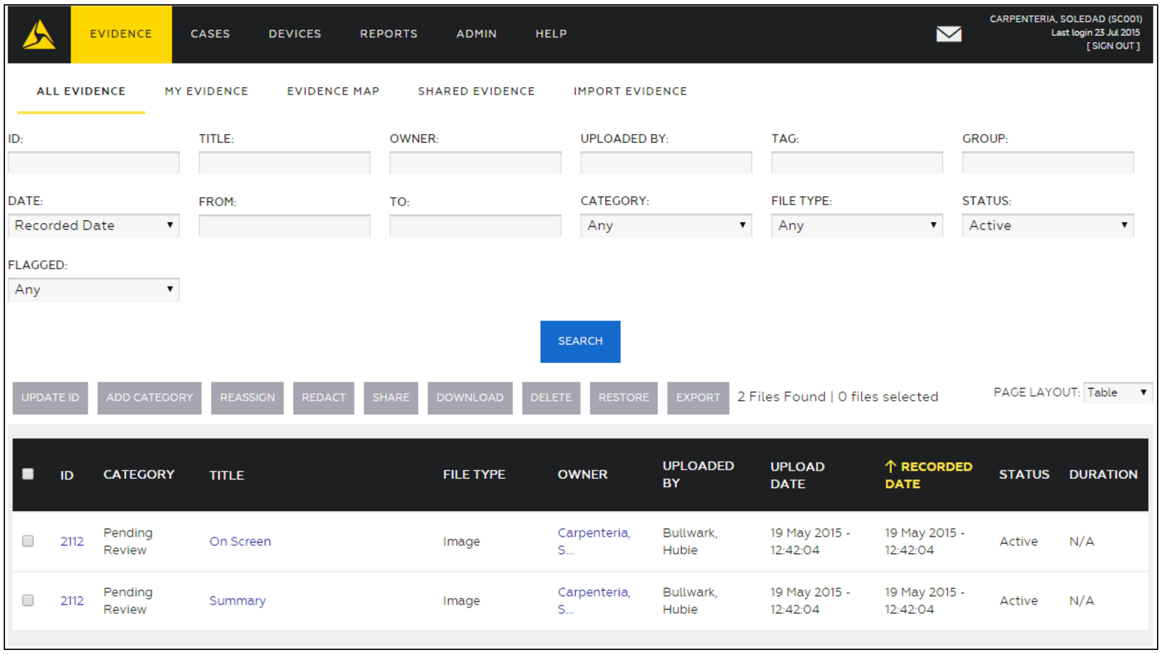
Evidence Search — All Evidence, My Evidence, and Shared Evidence

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

- **All Evidence** — Finds all evidence, including evidence that you do not have permission to view.

- **My Evidence** — Finds evidence that you own. The Owner filter is automatically set to your name.

- **Shared Evidence** — Finds evidence that has been shared with you by the evidence owner.



CARPENTERIA, SOLEDAD (SC001)
Last login 23 Jul 2015
[SIGN OUT]

ID:
TITLE:
OWNER:
UPLOADED BY:
TAG:
GROUP:
DATE: Recorded Date
FROM:
TO:
CATEGORY: Any
FILE TYPE: Any
STATUS: Active
FLAGGED: Any

2 Files Found | 0 files selected

PAGE LAYOUT: Table

□	ID	CATEGORY	TITLE	FILE TYPE	OWNER	UPLOADED BY	UPLOAD DATE	↑ RECORDED DATE	STATUS	DURATION
□	2112	Pending Review	On Screen	Image	Carpenteria, S...	Bullwark, Hubie	19 May 2015 - 12:42:04	19 May 2015 - 12:42:04	Active	N/A
□	2112	Pending Review	Summary	Image	Carpenteria, S...	Bullwark, Hubie	19 May 2015 - 12:42:04	19 May 2015 - 12:42:04	Active	N/A

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**.
Change search results	1. Update the evidence search filters. For more information, see Evidence Search Filters. 2. Click **Search**.
Sort search results	Click the column headings for **ID**, **Title**, **Uploaded Date**, or **Recorded Date**.
Switch between page layout options (table, detailed, or gallery)	On the **Page Layout** list, click the layout you want.

For information about the actions you can take from evidence search results, see Working with Evidence Search Results.

Evidence Search Filters

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

- **ID** — Limits search results to evidence whose ID includes the characters you enter in the ID box. For more information, see Text Search Details.
- **Title** — Limits search results to evidence whose title includes the characters you enter in the Title box. For more information, see Text Search Details.
- **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.
- **Date** — Limits search results by either the recorded, uploaded, or deletion date of evidence, as selected. You must also specify a date range by using the From and To boxes, else the search is not limited by date range. Search results are inclusive of the dates specified.
    - **From** — The start of the date range. If the From box is empty, the date range begins with the earliest possible date.
    - **To** — The end of the date range. If the To box is empty, the date range ends with today.
- **File Type** — Limits search results to the file type selected. By default, search results include all file types.
- **Owner** — Limits search results to evidence owned by the user specified. To specify the user, click in the Owner box, start typing the name of the user, wait for Evidence.com to show the matching users, and then click the user you want.

  On the My Evidence page, the Owner filter is set to your name by default.
- **Uploaded By** — Limits search results to evidence uploaded by the user specified. To specify the user, click in the Uploaded By box, start typing the name of the user, wait for Evidence.com to show the matching users, and then click the user you want.
- **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.
- **Tag** — Limits search results to evidence whose tags includes the characters you enter in the Tag box. For more information, see Text Search Details.

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

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

Text Search Details

For evidence searches, the ID, Title, and Tag filters provide advanced text matching features.

- The text you enter can match any part of the data you are filtering. For example, if you enter `21` in the ID box, any evidence whose ID includes "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. For example, if you enter `21 78` in the ID box, search results include evidence with the ID 213789 as well as 421278.

- 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 213789.

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.

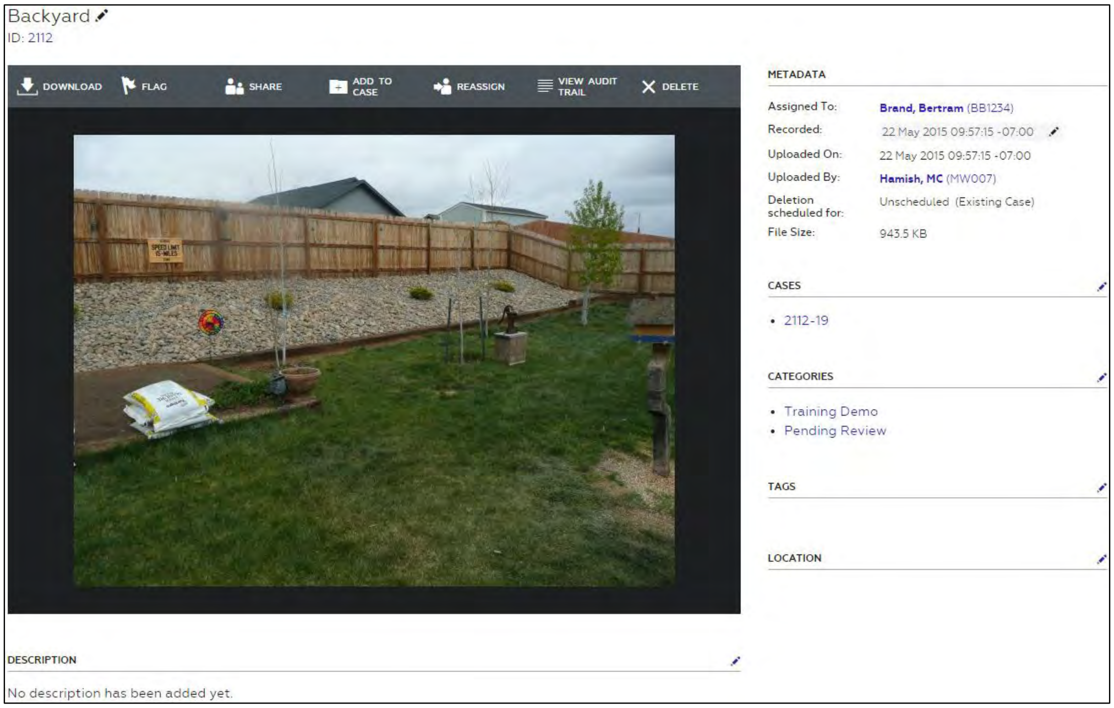
- You are an administrator.

1. Search for the evidence you want to view.

2. In the search results, click the title of the evidence.

The View Evidence page opens.

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



Backyard

ID: 2112

METADATA

Assigned To: **Brand, Bertram** (BB1234)

Recorded: 22 May 2015 09:57:15 -07:00

Uploaded On: 22 May 2015 09:57:15 -07:00

Uploaded By: **Hamish, MC** (MW007)

Deletion scheduled for: Unscheduled (Existing Case)

File Size: 943.5 KB

CASES

- 2112-19

CATEGORIES

- Training Demo
- Pending Review

TAGS

LOCATION

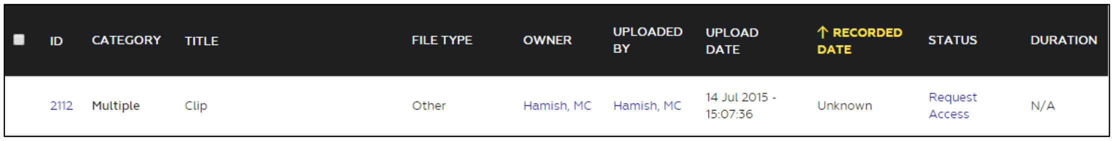
DESCRIPTION

No description has been added yet.

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**.



■	ID	CATEGORY	TITLE	FILE TYPE	OWNER	UPLOADED BY	UPLOAD DATE	↑ RECORDED DATE	STATUS	DURATION
	2112	Multiple	Clip	Other	Hamish, MC	Hamish, MC	14 Jul 2015 - 15:07:36	Unknown	Request Access	N/A

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 Share Evidence by Authenticated Sharing

Bulk sharing enables you to share more than one evidence file at a time.

Authenticated sharing enables you to share evidence with other users of Evidence.com. You should use authenticated sharing when you need to require that evidence is only available to users who sign in to Evidence.com. You can control whether users you share evidence with can view the evidence, download the evidence, view the audit trail of evidence, and share the evidence with others.

Bulk sharing evidence grants each user the same permissions to the shared evidence. If you need to grant different permissions to different users, perform this procedure once for each set of users to whom you want to grant the same permissions.

Removing a sharing invitation and changing sharing expiration date cannot be done in bulk. Instead, if you need to perform these tasks, you must perform them once for each evidence file. For more information, see Change Evidence Sharing Expiration Date and Remove an Evidence Sharing Invitation.

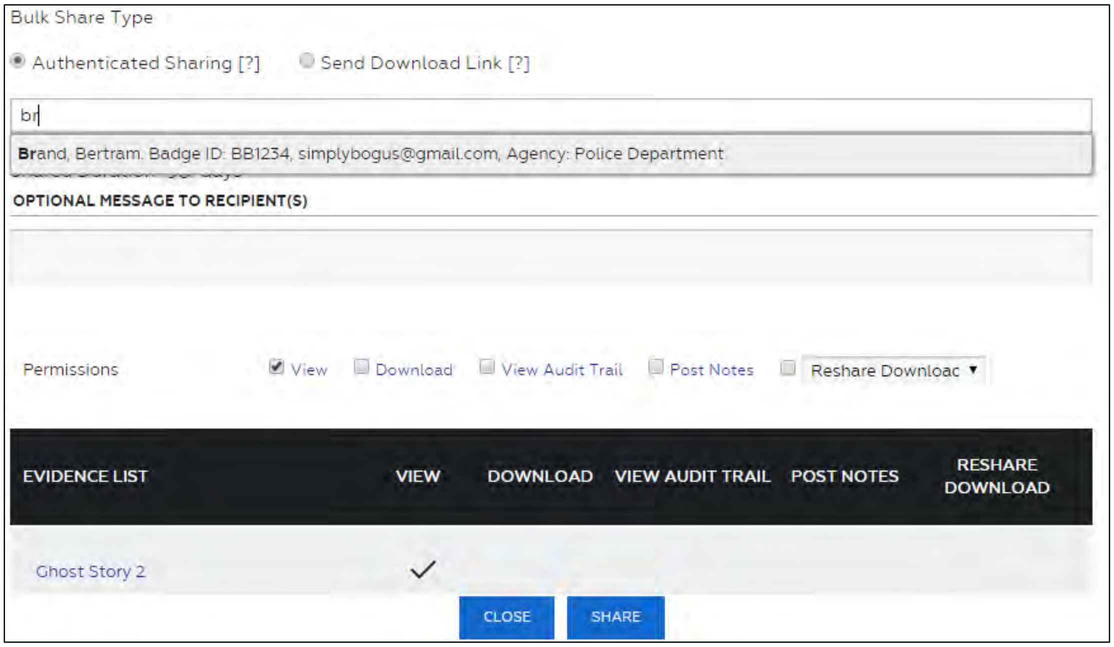
1. Search for the evidence you want to share.

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

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

   A dialog box displays the options for bulk sharing.

4. Under **Bulk Share Type**, click **Authenticated Sharing**.



Bulk Share Type

● Authenticated Sharing [?] ○ Send Download Link [?]

br

Brand, Bertram. Badge ID: BB1234, simplybogus@gmail.com, Agency: Police Department

OPTIONAL MESSAGE TO RECIPIENT(S)

Permissions ☑ View □ Download □ View Audit Trail □ Post Notes □ Reshare Downloac ▾

EVIDENCE LIST	VIEW	DOWNLOAD	VIEW AUDIT TRAIL	POST NOTES	RESHARE DOWNLOAD
Ghost Story 2	✓				

5. Use the first box to add the users with whom you want to share the evidence, as follows:

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

  The user you selected appears above the box. If the user is in your agency, the user has a white background. If the user is in a partner agency, the user has a green background.

- For a user who is not in your agency or a partner agency, type the email address of the user and then press **Enter**.

  If the user already has a my.evidence.com account, the email address appears above the box, with a yellow background.

  If the user does not have a my.evidence.com account, the email address remains in the first box. The user receives an invitation email; however, if you need to add more users, complete this procedure, and then repeat it until you have shared the evidence with all required users.

  After you complete the sharing process, the person receiving the sharing invitation can use my.evidence.com to view the evidence.

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

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

   - View — User is able to view the evidence.
   - Download — User is able to download a copy of the evidence to their hard drive.
   - Audit Trail — User is able to view the audit trail.
   - Post Notes — User is able to post notes to the evidence.
   - Reshare Download — User is able to forward the permission to download to other users.
   - Reshare All — User is able to forward all of their permissions to other users.

8. Click **Share** and then, on the confirmation message box, click **OK**.

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

Bulk Share by Unauthenticated Download Link

Bulk sharing enables you to share more than one evidence file at a time.

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

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

Note: If you want to require persons downloading evidence to sign in to Evidence.com, use authenticated bulk sharing and specify the permission to download the evidence. For more information, see Bulk Share Evidence by Authenticated Sharing.

1. Search for the evidence you want to share.

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

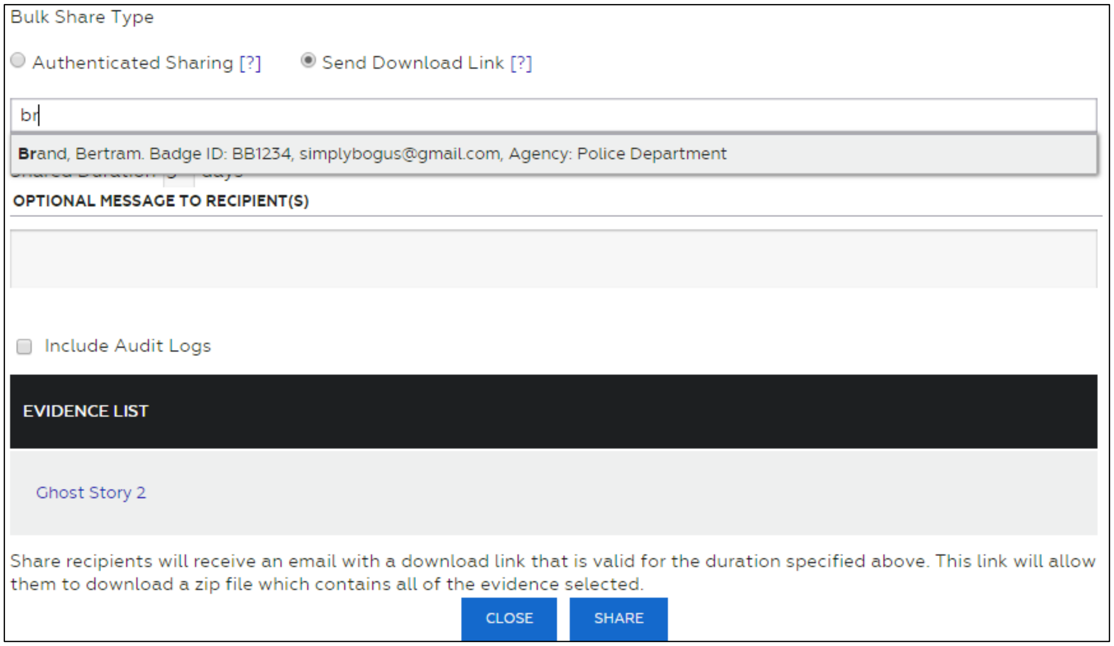
3. Above the search results, click **Share**.

   A dialog box displays the options for bulk sharing.

4. From the row of buttons above the search results, click **Share**.

A dialog box displays the options for bulk sharing.

5. Click **Send Download Link**.



Bulk Share Type

○ Authenticated Sharing [?] ● Send Download Link [?]

br

Brand, Bertram. Badge ID: BB1234, simplybogus@gmail.com, Agency: Police Department

OPTIONAL MESSAGE TO RECIPIENT(S)

□ Include Audit Logs

EVIDENCE LIST

Ghost Story 2

Share recipients will receive an email with a download link that is valid for the duration specified above. This link will allow them to download a zip file which contains all of the evidence selected.

6. Use the first box to add the users with whom you want to share the evidence, as follows:

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

  The user you selected appears above the box. If the user is in your agency, the user has a white background. If the user is in a partner agency, the user has a green background.

- For a user who is not in your agency or a partner agency, type the email address of the user and then press **Enter**.

  If the user already has a my.evidence.com account, the email address appears above the box, with a yellow background.

  If the user does not have a my.evidence.com account, the email address remains in the first box. The user receives an invitation email; however, if you need to add more users, complete this procedure, and then repeat it until you have shared the evidence with all required users.

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

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

8. If you want to include audit logs, check the corresponding check box.

9. Click **Share**.

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

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

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

Update ID

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

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

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

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

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

   A dialog box appears.

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

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

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

Add Category to Evidence

You can add a category to one or more evidence files in search results.

A category name can be up to 50 alphanumeric characters.

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

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

3. Above the search results, click **Add Category**.

   A dialog box appears.

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

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

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

Reassign Evidence

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

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

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

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

   A dialog box appears.

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

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

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

Bulk Video Redaction

Public disclosure requests can be time consuming, especially when large volumes of videos have to 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.

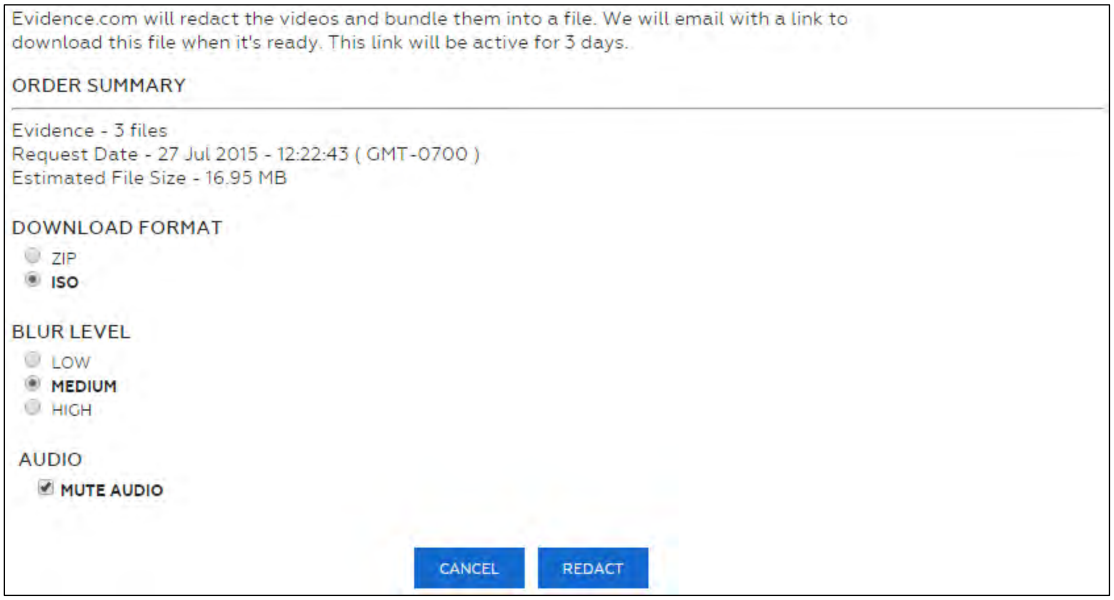
Note: If you need to redact a video more precisely, such as redacting only a portion of each video frame, see Video Evidence Redaction.

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

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

3. Click **Redact**.

   The Bulk Redaction dialog box appears.



Evidence.com will redact the videos and bundle them into a file. We will email with a link to download this file when it's ready. This link will be active for 3 days.

ORDER SUMMARY

Evidence - 3 files
Request Date - 27 Jul 2015 - 12:22:43 (GMT-0700)
Estimated File Size - 16.95 MB

DOWNLOAD FORMAT

○ ZIP
● **ISO**

BLUR LEVEL

○ LOW
● **MEDIUM**
○ HIGH

AUDIO

☑ **MUTE AUDIO**

4. Under **Download format**, click the file format in which you to receive the 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. If you want Evidence.com to remove all audio from the redacted video files, ensure that the **Mute audio** check box is selected.

7. If you want the original audio of all video files to be preserved in the redacted video files, click to clear the **Mute audio** check box.

8. Click **Redact**.

9. 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.

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

    A web browser opens your Evidence.com agency.

11. 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:

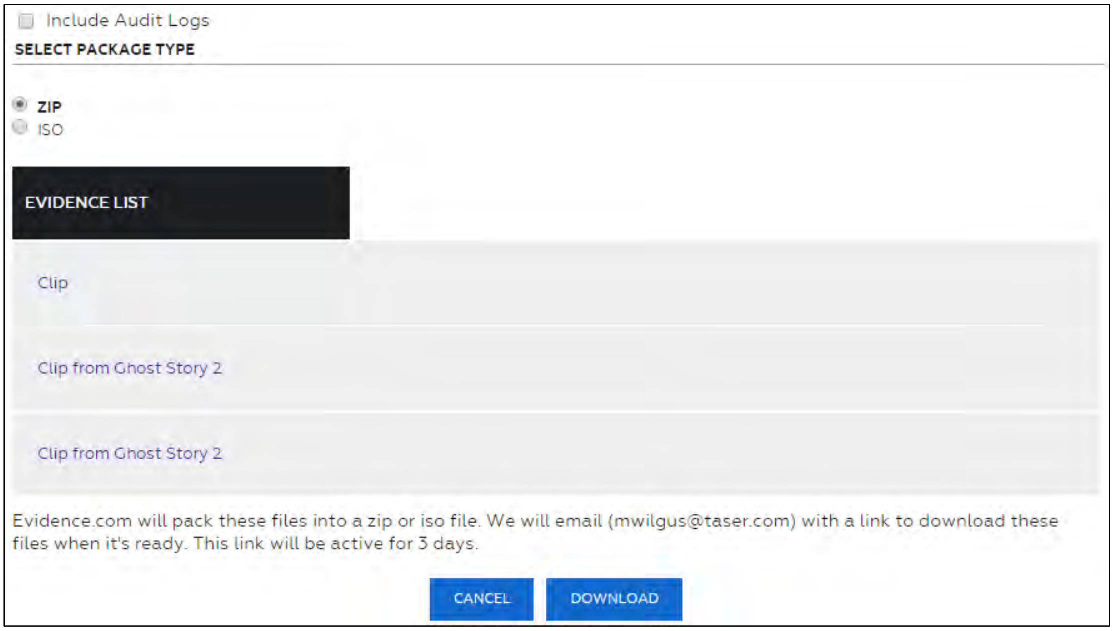
- ZIP — Evidence.com includes the selected evidence files in a ZIP file.
- ISO — Evidence.com includes the selected evidence files in an ISO image, which can be used to create a CD-ROM or DVD.

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 **Download**.

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



□ Include Audit Logs

SELECT PACKAGE TYPE

● ZIP
○ ISO

EVIDENCE LIST

Clip

Clip from Ghost Story 2

Clip from Ghost Story 2

Evidence.com will pack these files into a zip or iso file. We will email (mwilgus@taser.com) with a link to download these files when it's ready. This link will be active for 3 days.

4. If you want to include audit trails for the selected evidence files, click the **Include Audit Logs** check box.

5. Under **Select Package Type**, select the file type that you want for the download file.

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

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

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

   A web browser opens your Evidence.com agency.

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

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

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.

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.

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

1. Search for evidence and refine the search until the search results represent the evidence list that you want to export.
2. Above the search results, click **Export**.
3. In the **Select Format** list, click the file format that you want for the exported evidence list and then, on the message box, click **Export**.

   The evidence list downloads in the format that you specified.

   If the evidence search results contain more than 500 evidence files, only the first 500 files are included in the downloaded list and Evidence.com displays a dialog box for downloading the next 500 files in the search results.
4. If you want to export evidence lists for additional evidence, click **OK** each time the dialog box appears.

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

Working with Any Evidence

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

Actions available for video and audio files only are described in Working with Video and Audio Evidence.

Share an Evidence File

From the View Evidence page, you can share an evidence file with any of the following:

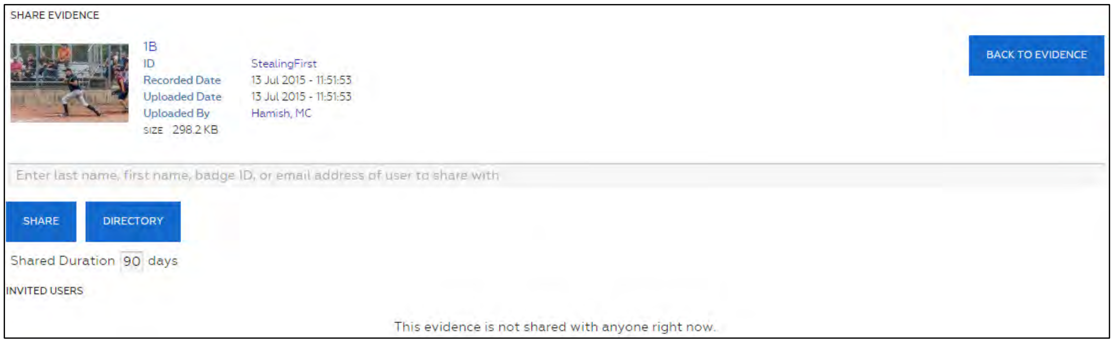
- Users in your agency
- Users in a partner agency
- Anyone who has an email address and who is willing to create a my.evidence.com user account

If you want to share more than one evidence file at a time, see Bulk Share Evidence by Authenticated Sharing.

On the View Evidence page, the Share button is above the evidence preview. If the evidence is already shared, the button text is “Shared (*N*)” where *N* is the number of users who the evidence is shared with.

1. Click **Share**.

   The Share Evidence page appears.



SHARE EVIDENCE

1B

ID	StealingFirst
Recorded Date	13 Jul 2015 - 11:51:53
Uploaded Date	13 Jul 2015 - 11:51:53
Uploaded By	Hamish, MC
SIZE	298.2 KB

Enter last name, first name, badge ID, or email address of user to share with

Shared Duration 90 days

INVITED USERS

This evidence is not shared with anyone right now.

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

3. If you want to share with users in your agency, click **Directory**; on the User Search dialog box, search for the users; select the check box next to each user; click **Add Users**; on the notification message box, click **OK**; and then click **Close**.

   On the Share Evidence page, the users you selected appear above the first box, with a white background.

4. If you want to share with users who you didn’t already add in the previous step, use the first box on the Share Evidence page, as follows:

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

     The user you selected appears above the box. If the user is in your agency, the user has a white background. If the user is in a partner agency, the user has a green background.

   - For a user who is not in your agency or a partner agency, type the email address of the user and then press **Enter**.

     The email address appears above the box, with a yellow background. After you complete the sharing process, the person receiving the sharing invitation can use my.evidence.com to view the evidence.

5. When you have finished adding all the users with whom you want to share this evidence, click **Share**.

   The Permissions dialog box lists the users you added and the sharing permissions available for each user.

6. For each user listed, select the sharing permissions that you want to grant to that user.

   - View — User is able to view the evidence.
   - Download — User is able to download a copy of the evidence to their hard drive.
   - View Audit Trail — User is able to view the evidence audit trail.
   - Post Notes — User is able to post notes to the evidence.
   - Reshare Download — User is able to forward the permission to download to other users.
   - Reshare All — User is able to forward all of their permissions to other users.

7. When you have finished selecting sharing permissions, click **OK**.

   On the Share Evidence page, the users you shared with are listed under Invited Users.

   Evidence.com sends each user a notification email about the shared evidence file.

   Users who do not have an Evidence.com account receive an email that invites them to register at my.evidence.com in order to gain access to the evidence.

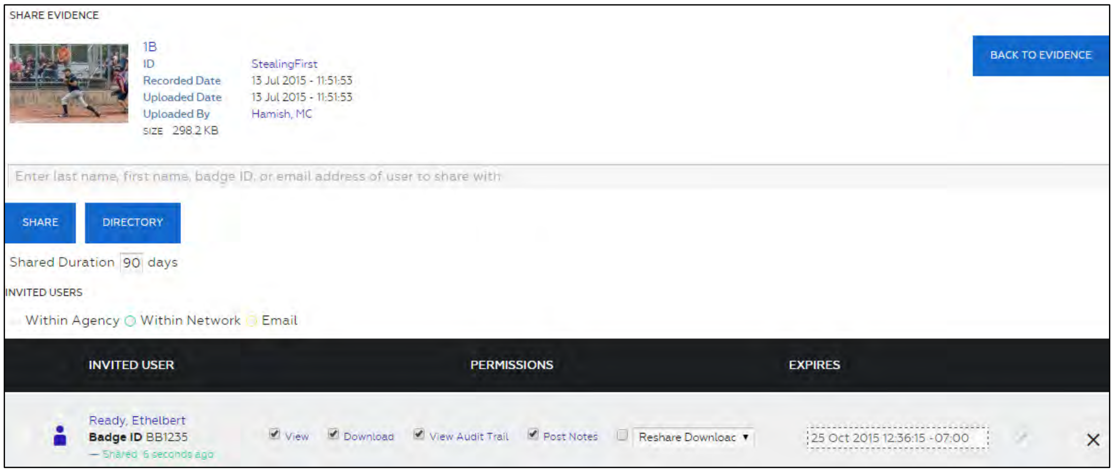
Change Evidence Sharing Expiration Date

Each user you share an evidence file with has a separate, editable sharing expiration date. The expiration date for shared evidence is determined initially by the shared duration that you specify when you share the evidence.

You can change a user's sharing expiration date for any shared evidence file. For example, if a user needs access to the evidence for longer than expected, you can change the sharing expiration date.

1. On the View Evidence page, click **Share**.

   On the Share Evidence page, the Invited Users area lists the users whom the evidence is shared with.



1B

ID StealingFirst
Recorded Date 13 Jul 2015 - 11:51:53
Uploaded Date 13 Jul 2015 - 11:51:53
Uploaded By Hamish, MC
SIZE 298.2 KB

Enter last name, first name, badge ID, or email address of user to share with

Shared Duration 90 days

○ Within Agency ○ Within Network ○ Email

INVITED USER	PERMISSIONS	EXPIRES
Ready, Ethelbert **Badge ID** BB1235 — Shared 6 seconds ago	☑ View ☑ Download ☑ View Audit Trail ☑ Post Notes □ Reshare Downloac ▾	25 Oct 2015 12:36:15 -07:00

2. Find the user whose sharing expiration date you want to change and click ✎ (edit) next to the date.

   A calendar appears.

3. Select the new date and click **OK**.

4. If you need to change the date, use the calendar tool to select the date.

5. If you need to change the time, use the sliders to set the hour, minute, and second.

6. If you need to change the time zone, on the **Time Zone** list, click the time zone.

7. After you finish editing the sharing expiration date and time, click **OK**.

   On the Share Evidence page, the user's new sharing expiration date appears on the Share Evidence page.

Remove an Evidence Sharing Invitation

If you no longer want to share evidence with a user, you can remove the user's sharing invitation. For example, if you shared evidence with the wrong user, you can remove the sharing invitation to ensure that the user cannot access the evidence.

Note: If a user in your agency has permission to view any evidence, removing an invitation to share evidence with the user does not affect the user's access to the evidence.

1. On the View Evidence page, click **Share**.

   On the Share Evidence page, the Invited Users area lists the users whom the evidence is shared with.

2. Find the user whose sharing invitation you want to revoke and, to the far right of the user name, click ✕ (remove).
3. On the confirmation message box, click **Continue**.
4. On the notification message box, click **OK**.

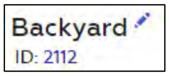
Edit Title and ID

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

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

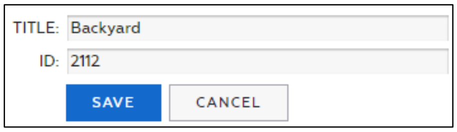
An evidence title can be up to 256 alphanumeric characters.

1. To the right of the evidence title, click ✎ (edit).



Backyard ✎
ID: 2112

The title and ID become editable.



TITLE: Backyard
ID: 2112

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

The View Evidence page shows the updated title and ID.

Edit Recorded Date and Time

On the View Evidence 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 View Evidence 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.

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 View Evidence 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.

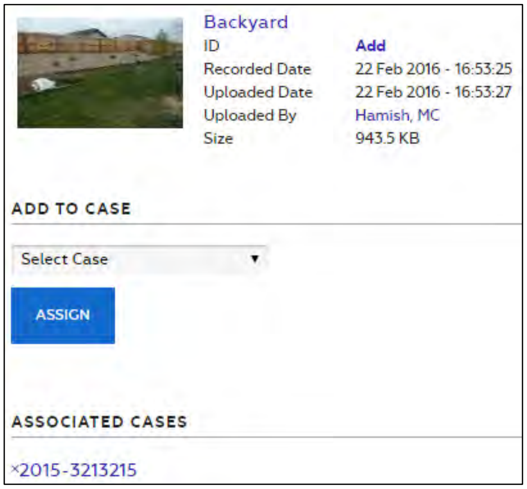
Add to or Remove Evidence from a Case

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

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

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

   The Add to Case page appears.



Backyard

ID	Add
Recorded Date	22 Feb 2016 - 16:53:25
Uploaded Date	22 Feb 2016 - 16:53:27
Uploaded By	Hamish, MC
Size	943.5 KB

ADD TO CASE

Select Case ▾

ASSIGN

ASSOCIATED CASES

×2015-3213215

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

   The case that you selected appears under Associated Cases.

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

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

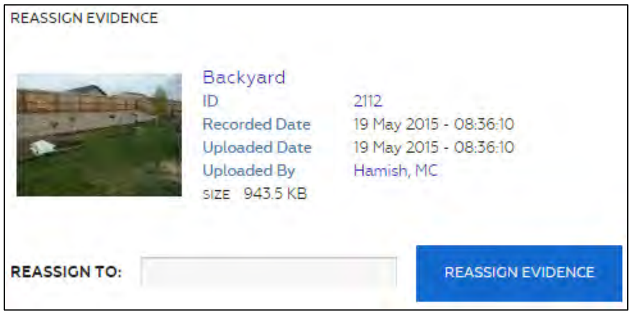
Reassign Evidence

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

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

1. Click **Reassign**.

   The Reassign Evidence page appears.



REASSIGN EVIDENCE

Backyard

ID 2112

Recorded Date 19 May 2015 - 08:36:10

Uploaded Date 19 May 2015 - 08:36:10

Uploaded By Hamish, MC

SIZE 943.5 KB

REASSIGN TO:

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

3. Click **Reassign**.

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

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

   The View Evidence page appears.

View Evidence Audit Trail

You can view the audit trail for an evidence file.

On the View Evidence 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 Log**, click **Submit**.

3. If you want to view a portion of the audit trail, under **View Portion of Audit Log**, 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 View Evidence 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.

On the View Evidence page for evidence that has the status of Deleting, the Restore button appears above the evidence preview.

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

   The evidence status becomes Active.

Assign and Un-Assign Categories

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

On the View Evidence page, the Categories area appears on the right side of the page. It lists the categories that the evidence is assigned to, if any.

1. 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 **Add**.

   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.

Extend Retention Period

If evidence is scheduled for deletion, you can extend how long Evidence.com retains the evidence before adding it to the deletion queue. The period of time that the retention is extended is equal to the length of the retention policy currently in effect for the evidence. The category assigned to the evidence determines the retention policy. If more than one category is assigned to evidence, the longest retention policy is applied.

For example, if an evidence file is assigned a category with a 30-day retention policy and deletion is scheduled 20 days from today, extending the retention period would reschedule deletion to 50 days from today.

On the View Evidence page, if the evidence is scheduled for deletion, the Extend Retention Period link appears on the right side of the page.

1. Click **Extend Retention Period**.

   A confirmation message box shows the new deletion date.

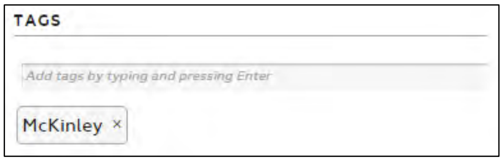
2. On the confirmation message box, click **OK**.

   The View Evidence page includes the updated deletion date.

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



A tag can be up to 256 alphanumeric characters.

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

Edit Location

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

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

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

   The Edit Location page shows a map.

2. In the **Jump to Address** box, type the location address and then click **Go**.

   The map shows the location you entered.

3. If you want to add notes about the location, in the **Additional Details** box, type the notes.

4. Click **Save**.

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

   The View Evidence page appears. Under Location, the small map shows the location that you specified.

Edit Description

You can add or edit a description of the evidence.

On the View Evidence 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 View Evidence 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.

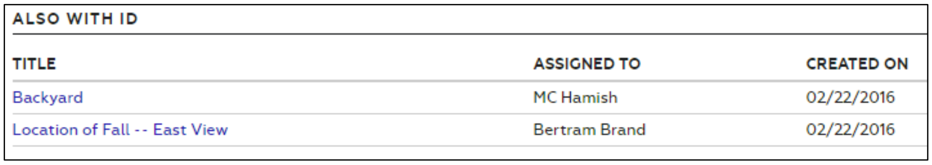
1. If necessary, scroll down and find the Notes area.
2. To the right of the note, click **X**.
3. On the confirmation dialog box, click **OKAY**.

   The note no longer appears on the View Evidence 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.



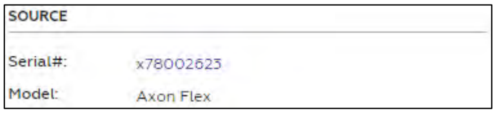
ALSO WITH ID

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 View Evidence 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

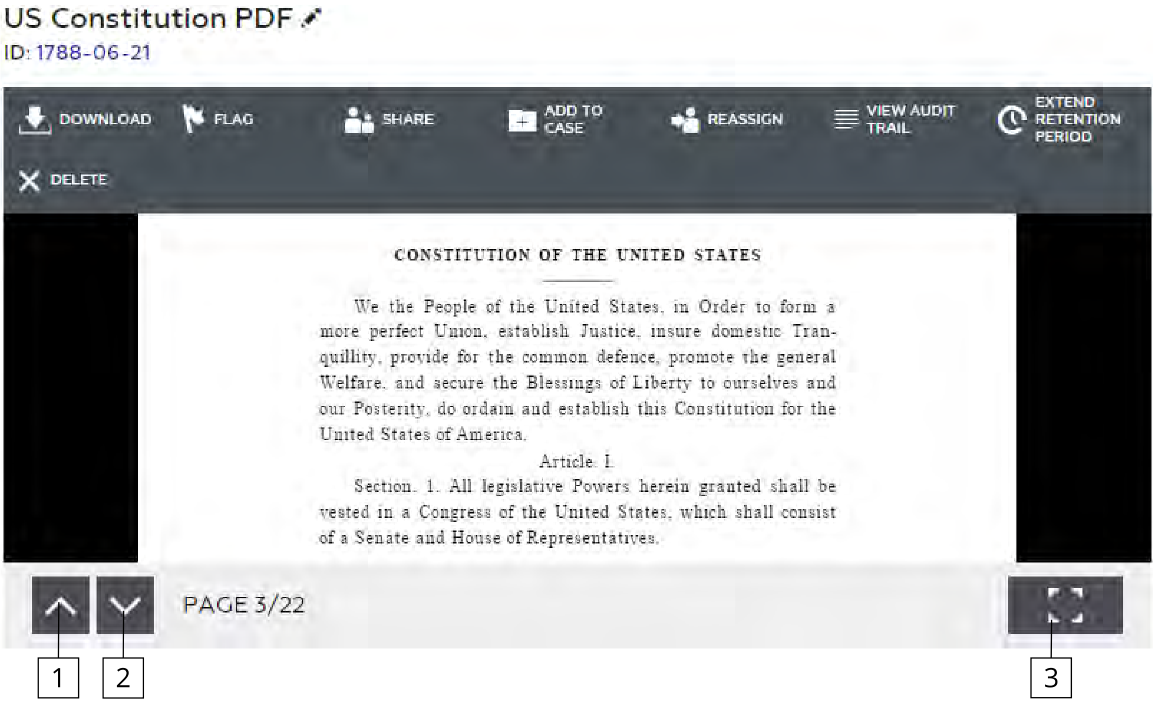
Serial#:	x78002623
Model:	Axon Flex

Viewing Document Evidence

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

PDF Viewer Controls

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



CONSTITUTION OF THE UNITED STATES

We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America.

Article. I.

Section. 1. All legislative Powers herein granted shall be vested in a Congress of the United States, which shall consist of a Senate and House of Representatives.

PDF Viewer Controls		
1 — Page up	2 — Page down	3 — Full screen

PDF Viewer Actions

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

Action	Steps
Page down	Click ∨ or press the down arrow key.
Page up	Click ∧ or press the up arrow key.
View Full Screen	To enter full-screen viewing mode, click ⛶. To exit full-screen viewing mode, click ✕.

Playing Video and Audio Evidence

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

Supported File Types

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

Video File Extension	Video Mime Type
.avi	video/avi
.fli	video/x-fli
.mov	video/quicktime
.movie	video/x-sgi-movie
.mpe	video/mpeg
.mpeg	video/mpeg
.mpg	video/mpeg
.qt	video/quicktime
.m4v	video/x-m4v
.webm	video/webm
.ogv	video/ogv
.mp4	video/mp4
.wmv	video/x-ms-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 file types supported by the Evidence.com media player include the types listed in the following table.

Audio File Extension	Audio Mime Type
.aif	audio/x-aiff
.aifc	audio/x-aiff
.aiff	audio/x-aiff
.au	audio/basic
.kar	audio/midi
.mid	audio/midi

Audio File Extension	Audio Mime Type
.midi	audio/midi
.mp2	audio/mpeg
.mp3	audio/mpeg
.mpga	audio/mpeg
.ra	audio/x-realaudio
.ram	audio/x-pn-realaudio
.rm	audio/x-pn-realaudio
.rpm	audio/x-pn-realaudio-plugin
.snd	audio/basic
.tsi	audio/TSP-audio
.wav	audio/x-wav

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

Internet Connection Speed Recommendations

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

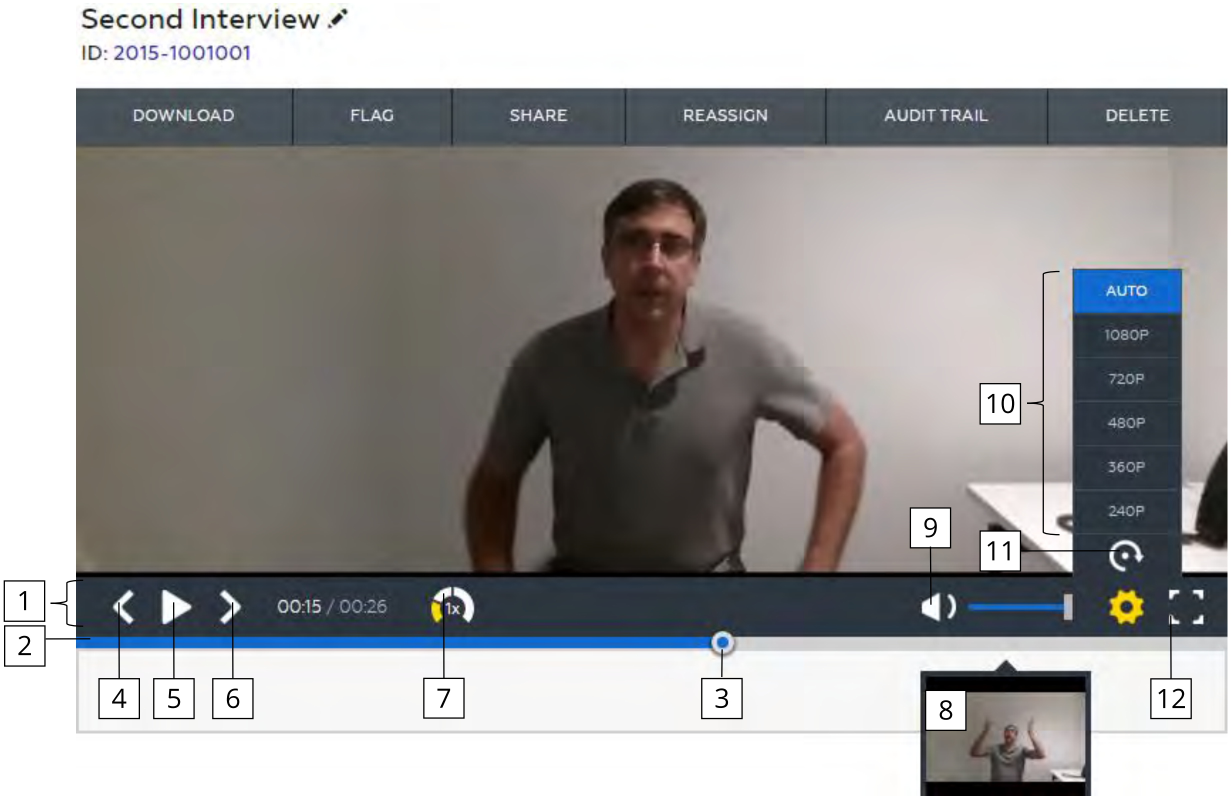
Resolution	Recommended Minimum Speed
480p	3 Megabits per second
720p	6 Megabits per second
1080p	10 Megabits per second

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

Media Player Controls

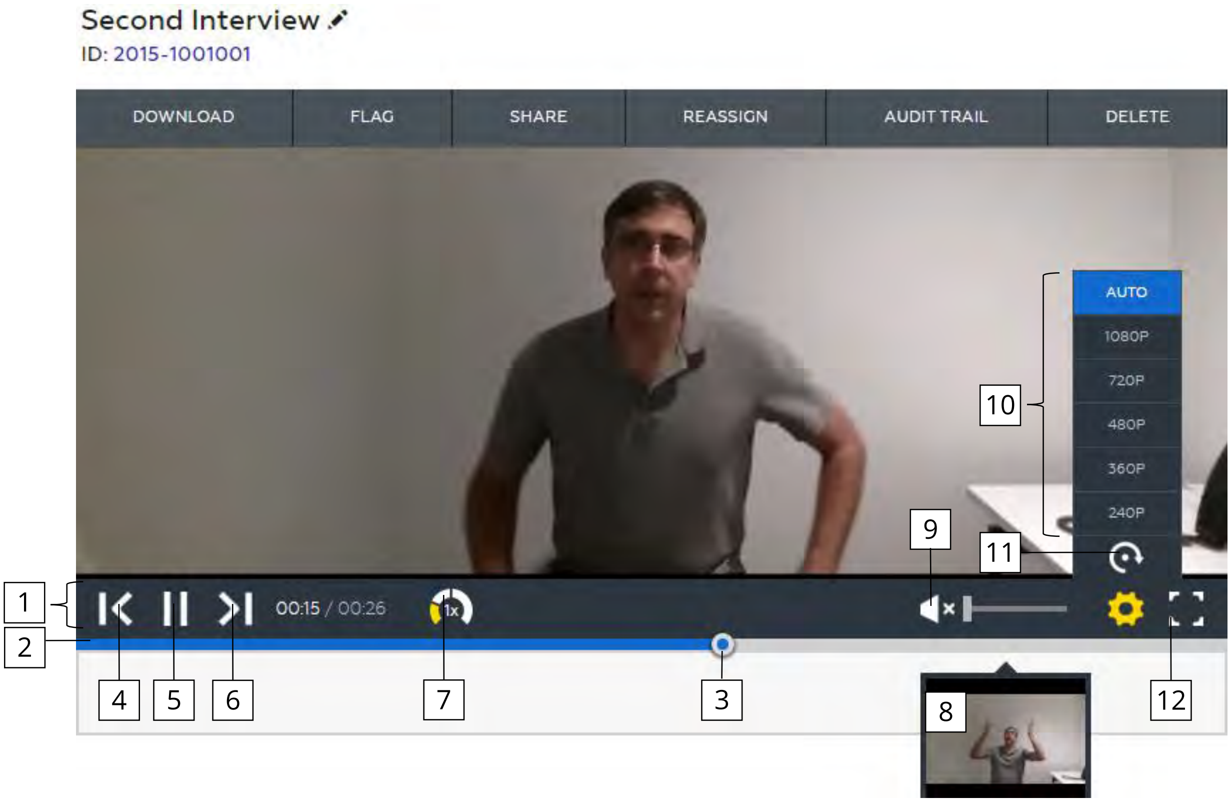
The Evidence.com media player enables you to play audio and video evidence files that are in supported file types.

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



Available Controls —Player Paused, Sound Unmuted	
1 — Playbar	7 — Playback speed selector
2 — Scrub bar	8 — Thumbnail
3 — Scrub handle	9 — Mute
4 — Previous frame	10 — Video quality selector
5 — Play	11 — Rotate
6 — Next frame	12 — Full screen

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



Second Interview

ID: 2015-1001001

Available Controls —Player Playing, Sound Muted	
1 — Playbar	7 — Playback speed selector
2 — Scrub bar	8 — Thumbnail
3 — Scrub handle	9 — Mute
4 — Previous event	10 — Video quality selector
5 — Pause	11 — Rotate
6 — Next event	12 — Full screen

Media Player Actions

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

Action	Steps
Play	Click ▶
Play faster or slower	Click the playback speed selector until the speed you want is selected. You can choose from standard speed (1X), double speed (2X), or quadruple speed (4X).
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 to Events	Click ❙❮ or ❯❙ The video jumps to the previous or next marker or clip.
Pause	Click ❚❚
View Frame by Frame	Click ❮ or ❯.
View Full Screen	To enter full-screen viewing mode, click ⛶. To exit full-screen viewing mode, click ✕.
Rotate Screen	1. Click ⚙. 2. Click ⟲.
Change video quality	1. Click ⚙. 2. Click the video quality that you want.
Mute, Unmute, or Control Volume	To mute audio, click 🔈. To unmute audio, click 🔇. To raise or lower the audio volume, click and hold the audio slider and drag it left (quieter) or right (louder), as needed.

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:

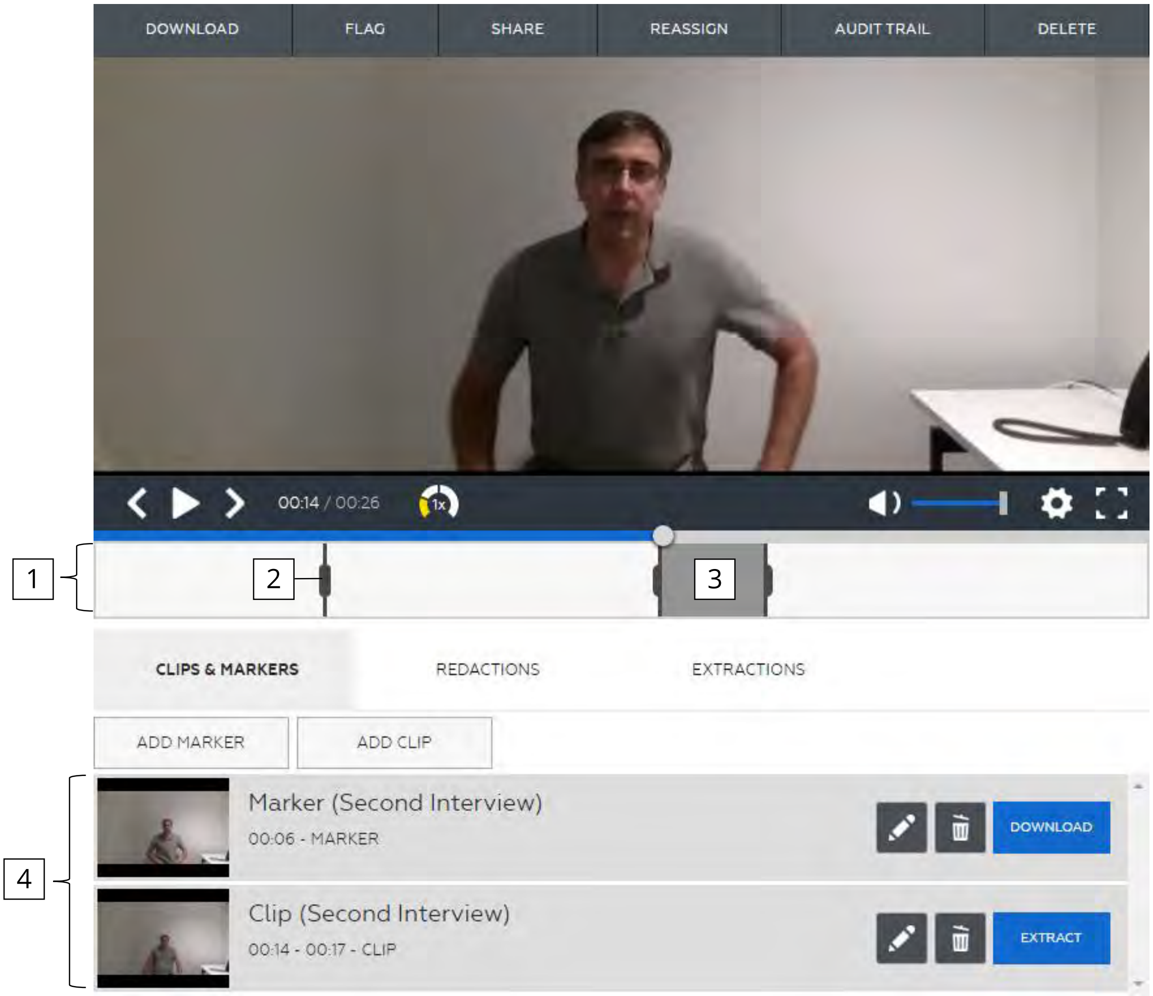
  - You can easily find important moments when you play the evidence file later.
  - Users with whom you share the evidence can easily locate moments that you have marked and read the title and description of the marker.
  - For video evidence only, you can download the marker as a picture file and send 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 (Second Interview)
00:06 - MARKER

Clip (Second Interview)
00:14 - 00:17 - CLIP

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

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

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

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

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

3. Click **Add Marker**.

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

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

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

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

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

View a Marker

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

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

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

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

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

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

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

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

Download a Marker

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

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

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

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

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

3. Click **Download**.

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

Add a Clip

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

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

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

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

2. Click **Add Clip**.

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

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

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

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

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

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

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

Play a Clip

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

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

1. On the View Evidence 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 View Evidence 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.	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.

Action	Steps
Move both handles together.	1. On the timeline, hover the mouse pointer over the blue area between the start and end handles. 2. Press and hold the mouse button. 3. Drag the handles left or right, as needed. 4. Release the mouse button.

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

   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 View Evidence 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 View Evidence 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 **OK**.

   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 View Evidence page, below the player, click **Clips & Markers**.

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

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

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

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

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

Video Evidence Redaction

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

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 either Evidence.com redaction tool:

- Manual redaction
- Assisted redaction featuring Smart Tracker technology

When you have completed creating or editing a redaction, you can extract a redacted video.

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.

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.

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 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.

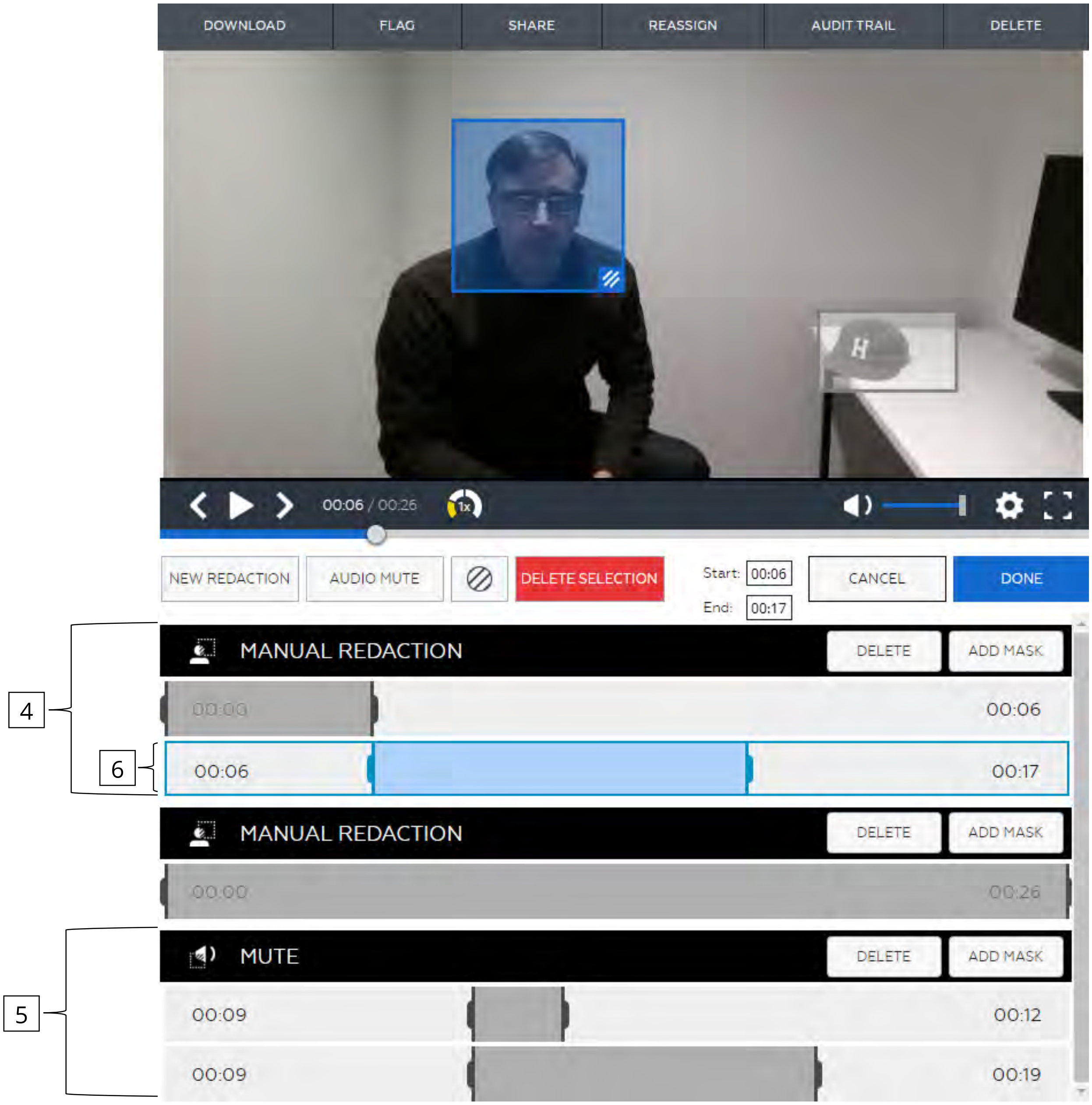
- **Object**—Organizes mask segments that redact the same actual object. A redaction contains one or more objects. Manual redaction supports two types of objects:
    - **Video object**—Organizes mask segments that redact one visual object. A video object contains one or more mask timelines.
    - **Mute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

Assisted Redaction

Assisted redaction, featuring Smart Tracker technology, 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.

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 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.

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.

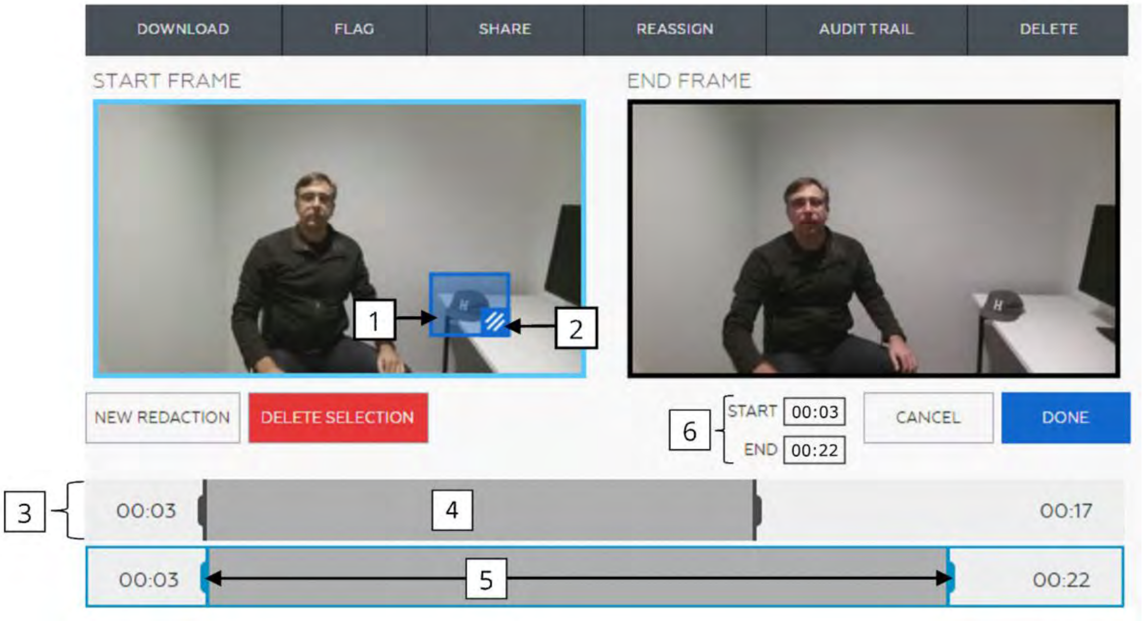
Because Smart Tracker technology automatically tracks objects in the video file, the assisted redaction feature represents an object and its timeline with one control, eliminating the need for you to create multiple mask timelines per object.

- **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.

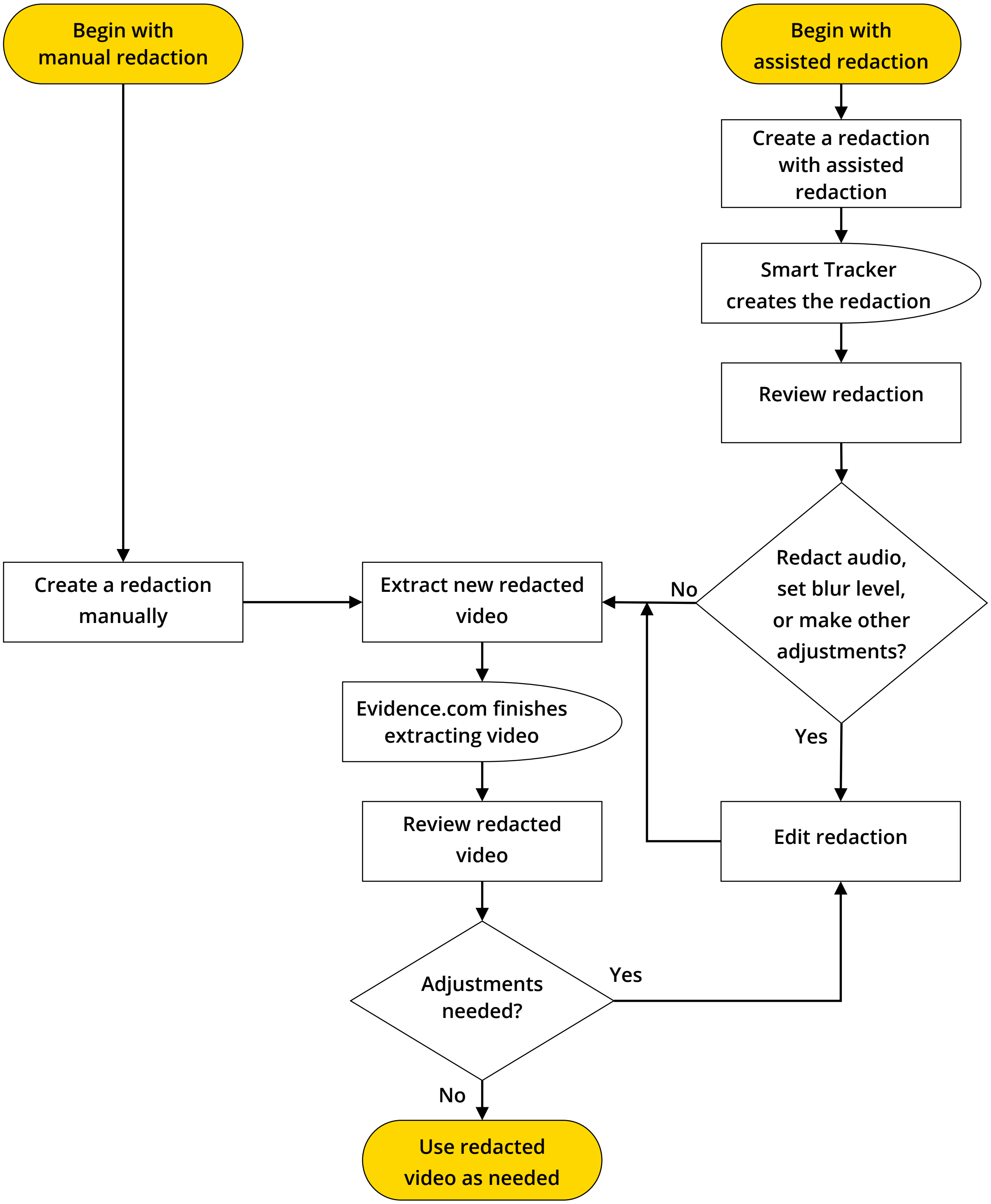
Assisted Redaction Controls



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 assisted redaction.


Begin with manual redaction
Begin with assisted redaction
Create a redaction with assisted redaction
Smart Tracker creates the redaction
Review redaction
Redact audio, set blur level, or make other adjustments?
No
Yes
Create a redaction manually
Extract new redacted video
Evidence.com finishes extracting video
Review redacted video
Edit redaction
Adjustments needed?
Yes
No
Use redacted video as needed

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 View Evidence page, below the video player, click **Redactions**.

   The Smart Tracker and Manual Redaction buttons appear below the Redactions tab. If any redactions already exist, they are listed below the buttons.

2. Click **Manual Redaction**.

   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.

3. 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**.

4. 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.

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

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

6. 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. Regardless of the origin of a redaction — created manually or created with assisted redaction — editing a redaction is the same process.

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

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	1. If the mask segment is not blue, click the mask segment. Blue indicates that the mask segment is selected. 2. Click **Delete Selection**.
Move the start or end mask segment handle	To place a mask handle approximately at the frame you need: 1. On the mask timeline, hover the mouse pointer over the mask segment handle that you want to move. 2. Press and hold the mouse button. 3. Drag the handle left or right, as needed. 4. Release the mouse button. To place a mask handle precisely at the frame you need: 1. If the mask segment is not blue, click the mask segment. Blue indicates that the mask segment is selected. 2. Use the keyboard controls, as needed: o The "a" key — Move the start handle to the left, one frame at a time. o The "s" key — Move the start handle to the right, one frame at a time. o Left Arrow key — Move the end handle to the left, one frame at a time. o Right Arrow key — Move the end handle to the right, one frame at a time.
Move both mask segment handles together	1. On the mask timeline, if the area between the mask segment handles is not blue, click between the handles. 2. Hover the mouse pointer over the blue area between the start and end handles. 3. Press and hold the mouse button. 4. Drag the handles left or right, as needed. 5. Release the mouse button.
Move mask segment handles to specific times	1. If the mask segment is not blue, click the mask segment. Blue indicates that the mask segment is selected. 2. In the **Start** box, enter the exact time in minutes and seconds, in *mm:ss* format, where you want the start handle. 3. In the **End** box, enter the exact time in minutes and seconds, in *mm:ss* format, where you want the end handle.
Move a mask frame in a mask segment	1. If the mask segment is not blue, click the mask segment in order to ensure that you are moving the correct mask frame. In the player, the 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.

Action	Method
Shape a mask frame	1. Click the mask segment in order to ensure that you are shaping the correct mask frame. In the player, the mask frame for the selected segment is red. 2. At the lower-right corner of the frame, click and hold the handle. 3. Drag the corner to where you want it. 4. Release the mouse button.
Change the blur level of a mask	1. Click the mask segment in order to ensure that you are setting the blur level for the correct mask. In the player, the frame for the selected segment is blue. 2. Click the blur selector until the blur level you want is selected. You can select Light, Normal, Heavy, or Blackout.

5. When you have finished editing the redaction objects, mask segments, and mask frames, do one of the following actions:

   - If you want to save all your edits to the redaction, click **Done**.

     Evidence.com saves the changes to the redaction.

   - If you do not want to save any edits to the redaction, click **Cancel**.

     Evidence.com discards any changes made to the redaction.

   The Redactions tab reappears.

Create a Redaction with Assisted Redaction

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

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 View Evidence page, below the video player, click **Redactions**.

   The Smart Tracker and Manual Redaction buttons appear below the Redactions tab. Below the buttons, any existing redactions are listed.

2. Click **Smart Tracker**.

   The assisted redaction controls replace the media player. Evidence.com creates the first object timeline for you. The timeline has one mask segment.

3. 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**.

4. 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	To place a mask handle approximately at the frame you need: 1. On the mask timeline, hover the mouse pointer over the mask segment handle that you want to move. 2. Press and hold the mouse button. 3. Drag the handle left or right, as needed. 4. Release the mouse button. To place a mask handle precisely at the frame you need: 1. If the mask segment is not blue, click the mask segment. Blue indicates that the mask segment is selected. 2. Use the keyboard controls, as needed: o The “a” key — Move the start handle to the left, one frame at a time. o The “s” key — Move the start handle to the right, one frame at a time. o Left Arrow key — Move the end handle to the left, one frame at a time. o Right Arrow key — Move the end handle to the right, one frame at a time.
Move both mask segment handles together	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	1. If the mask segment is not blue, click the mask segment. Blue indicates that the mask segment is selected. 2. In the **Start** box, enter the exact time in minutes and seconds, in *mm:ss* format, where you want the start handle. 3. In the **End** box, enter the exact time in minutes and seconds, in *mm:ss* format, where you want the end handle.

Action	Method
Move the mask frame in a mask segment	1. If the mask segment is not blue, click the mask segment in order to ensure that you are moving the correct mask frame. In the player, the mask frame 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	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.

5. 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 View Evidence 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 View Evidence 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 **OK**.

   Evidence.com begins creating the new redacted video evidence file.

   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 View Evidence 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.

View Videos Extracted from Clips 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 View Evidence page of the *parent* file.

2. Below the media player, click the **Extractions** tab.

   A gallery of extracted files appears below the Extractions tab.

3. Click the extracted file that you want to view.

   The View Evidence page of the extracted file opens.

4. Take the actions that you need. For more information, see Media Player Actions.

5. If you want to return to the View Evidence 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

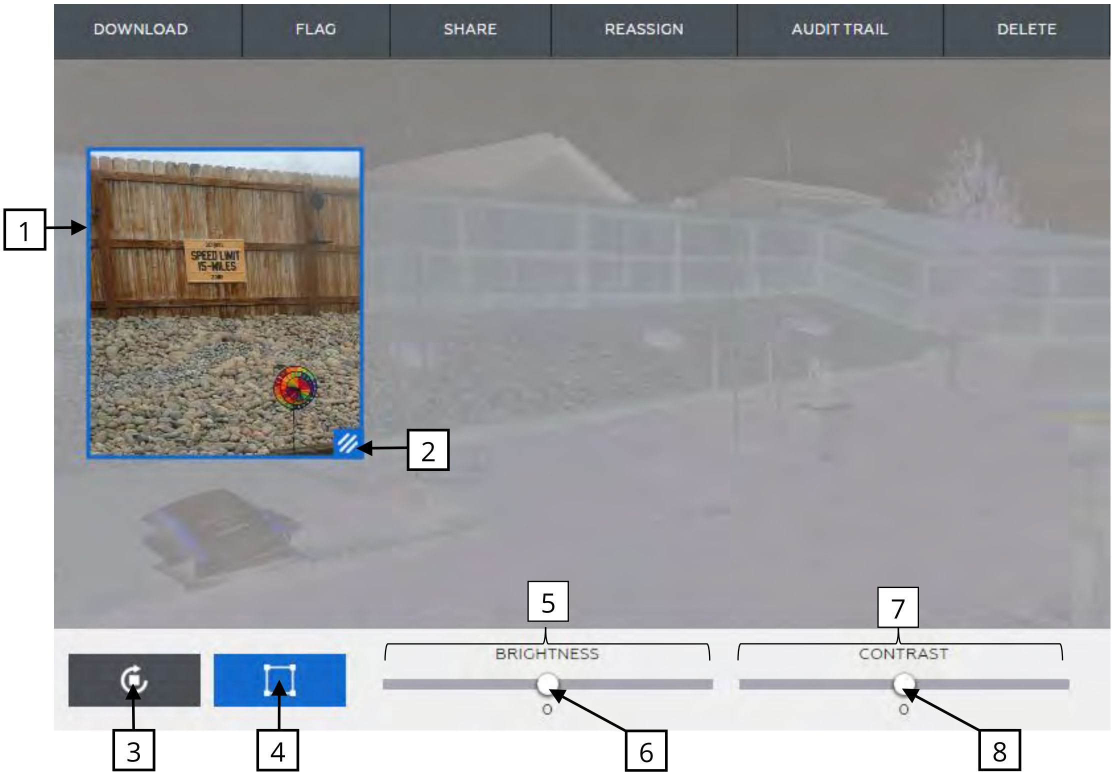
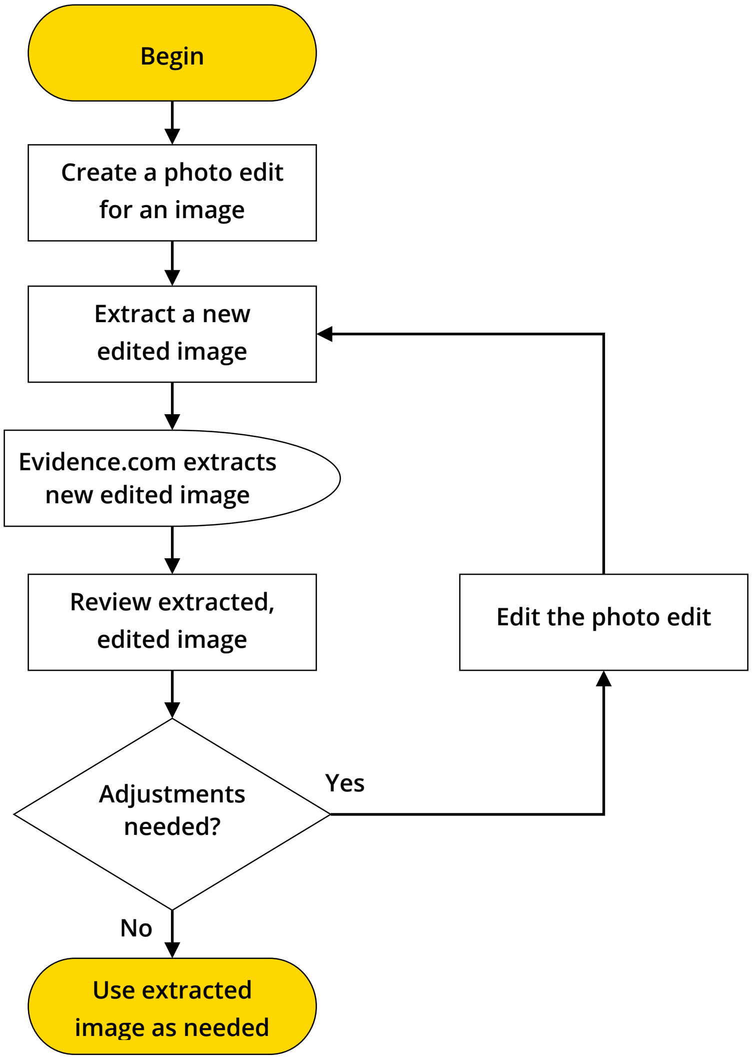


Image Tool Controls	
1 — Cropping frame	5 — Brightness slider
2 — Cropping frame handle	6 — Brightness slider handle
3 — Rotate	7 — Contrast slider
4 — Crop	8 — Contrast slider handle

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.


Begin
Create a photo edit for an image
Extract a new edited image
Evidence.com extracts new edited image
Review extracted, edited image
Adjustments needed?
Yes
Edit the photo edit
No
Use extracted image as needed

Create a Photo Edit

Administrators and users who are allowed the Evidence Edit permission can use the photo edit tool to create an edited image from an image evidence file that is in a file format supported by the media player.

1. On the View Evidence 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	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	1. Click ⛶. The cropping frame appears over the image. The area inside the cropping frame is what appearz 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	1. On the brightness slider, click and hold the slider handle. 2. Drag the handle left or right, until the brightness is at the level that you need. 3. Release the mouse button.
Adjust contrast	1. On the contrast slider, click and hold the slider handle. 2. Drag the handle left or right, until the contrast is at the level that you need. 3. Release the mouse button.

4. 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 View Evidence 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	1. To rotate the image 90 degrees clockwise, click ↻. 2. If you want to rotate the image more, continue clicking ↻ until the image is rotated as needed.
Remove image cropping	Click □. The cropping frame no longer appears on the image.
Adjust image cropping	If the cropping frame does not appear on the image, click □. To adjust the *position* of the cropping frame: 1. Click and hold the cropping frame, avoiding the handle at the lower-right corner of the frame. 2. Drag the frame to where you want it. 3. Release the mouse button. To adjust the *shape or size* of the cropping frame: 1. At the lower-right corner of the frame, click and hold the cropping frame handle. 2. Drag the corner to where you want it. 3. Release the mouse button.
Adjust brightness	1. On the brightness slider, click and hold the slider handle. 2. Drag the handle left or right, until the brightness is at the level that you need. 3. Release the mouse button.
Adjust contrast	1. On the contrast slider, click and hold the slider handle. 2. Drag the handle left or right, until the contrast is at the level that you need. 3. Release the mouse button.

4. Click **Done**.

   Evidence.com saves the changes you made to the photo edit.

Extract an Edited Image

After you create a photo edit, you can extract an edited image from it at any time. Extracting an edited image creates a new image evidence file that is edited exactly how you specified when you created the photo edit. Image evidence created by extracting an edited image appears in evidence searches. You can share or download the extracted edited image as needed, without affecting or sharing the original image evidence.

You can extract an edited image from a photo edit more than once. Each time you extract an edited image, a new image file is created. If the title of the photo edit is the same each time you extract an image from the photo edit, the image files created have identical titles.

An image extracted from a photo edit inherits the case IDs, categories, tags, and evidence location of the original image. Inheriting this information helps ensure that extracted images are associated with the correct cases and that the applicable evidence retention policy is enforced, including any restricted categories.

On the View Evidence 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 View Evidence 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 **OK**.

   Evidence.com begins creating the new edited image file.

   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 pin icons for any evidence that has location information. For more information, see Edit Location.

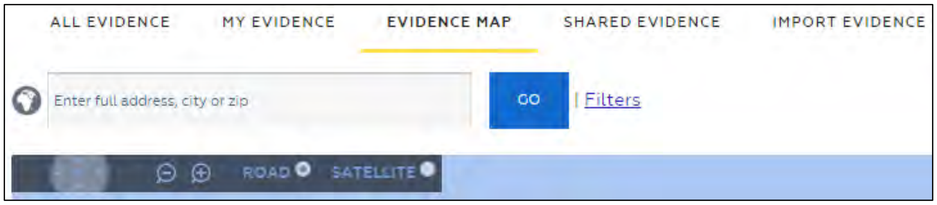
The map pin style used for an evidence file is determined by the category assigned to the evidence.

To view the evidence map, on the menu bar, click **Evidence** and then click **Evidence Map**.

The following sections describe the actions that you can take on the evidence map.

Basic Map Actions

The evidence map provides basic features for finding and viewing a location on the map. Many of these actions involve the map tool bar, shown in the following figure.



The following table describes the basic actions that are available on the evidence map.

Action	Steps
Pan	At the left end of the map tool bar, click the directional pad in the direction that you want to pan the map. Alternately, do the following steps: 1. Position the mouse pointer over the map. 2. Click and hold the mouse button. 3. Move the mouse to pan the map.
Zoom In or Zoom Out	1. In the map tool bar, hover the mouse pointer over the magnifying glass icons. 2. Use the slider to zoom in or out. Alternately, if your mouse has a mouse wheel: 1. Position the mouse pointer over the map. 2. Rotate the mouse wheel to zoom in or out.
Road View	In the map tool bar, click **Road**.
Satellite View	In the map tool bar, click **Satellite**.
Go to an Address	In the box above the map tool bar, type the address and then click **Go**.

Evidence Actions

Below the map, a table of evidence shown on the map appears. From the table of evidence, you can perform the following actions:

Action	Steps
Search for Evidence with Same ID	In the ID column, click the evidence ID that you want to search for. The All Evidence page opens, with search results filtered to the ID that you clicked.
View Evidence Page	If you have permission to view evidence, in the Title column, click the title of the evidence that you want to view. The View Evidence page opens.
Request Access to Evidence	If you do not have permission to view evidence: 1. In the Actions column for the evidence that you want to view, click **Request Access**. 2. If you want to include a message to the evidence owner, type it in the **Message** box. 3. Click **Send**. 4. On the notification message box, click **OK**.
View Evidence Owner	In the Owner column, click the user whose profile you want to view. The User Profile page opens.
View Evidence Audit Trail	1. In the Actions column for the evidence, click ≣ (view audit trail). 2. If you want to view the whole audit trail, under **View entire audit log**, click **Submit**. 3. If you want to view a portion of the audit trail, under **View portion of audit log**, specify a date in either or both the **From** or **To** boxes and click **Submit**. 4. Save or view the audit trail PDF as needed.
Download Evidence	1. In the Actions column for the evidence, click ⤓ (download evidence). 2. Under **Filename**, click the evidence file name. 3. Click **Close**.
Flag or Un-flag Evidence	In the Actions column for the evidence, click ⚑ (flag).
Delete Evidence	In the Actions column for the evidence, click ✕ (delete evidence).

Filtering the Evidence Map

1. Above the map, click **Filters**.

   The filters dialog box appears.

2. Specify the filters that you want to apply.

Filter	Steps
Date	1. Click in the **From** or **To** box. 2. Select the date. 3. Click **Filter**.
Officer	4. Click in the **Name** box. 5. Start typing the name of the user. 6. Wait for Evidence.com to show the matching users. 7. Click the user you want.
Category	Select the categories that you want to include on the evidence map.

3. If you want to remove a filter, click **Clear**.

4. Click **OK**.

   The evidence map shows only the evidence that matches the filters that you specified.

Case Management

Cases allow your agency to organize related evidence files, such as files that pertain to the same incident. Users can share cases with other users.

Case management features are available only in Evidence.com PRO agencies. In LITE agencies, the Case menu is unavailable.

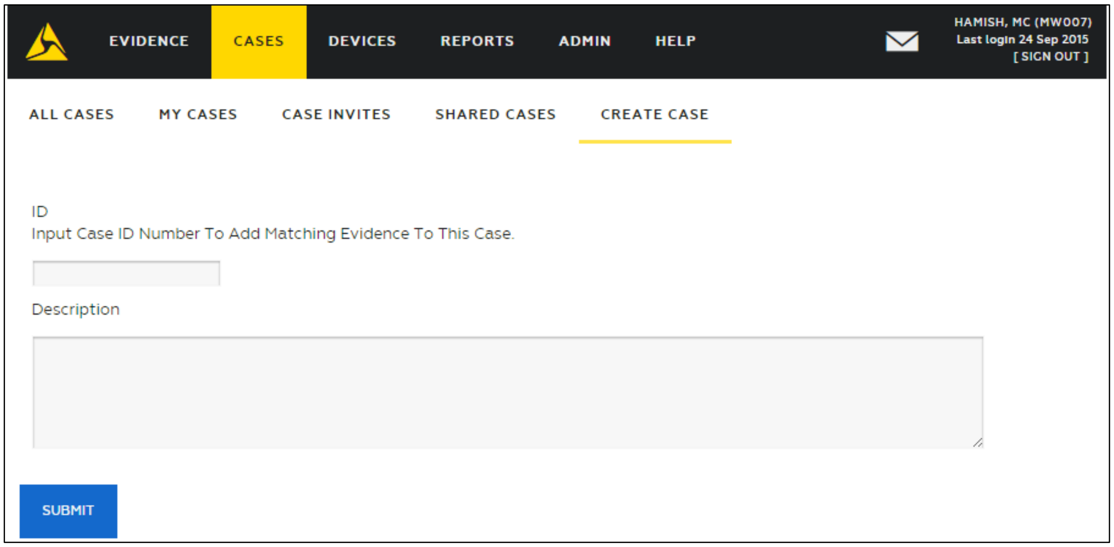
Create Case

Administrators and users whose role is allowed the Create Case permission can create a case.

The Add Matching Evidence feature makes it easy to add evidence to a case while you are creating the case. The feature finds evidence files that have the same ID that you specify for the case.

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

   The Create Case page appears.



2. Enter the case ID and double-check that it is correct.

3. Enter a useful description, and then click **Submit**.

   Evidence.com searches for evidence files that have the same ID as the ID you specified for the case. The Add Matching Evidence page lists 40 evidence files at a time. By default, all evidence is selected.

4. On the Add Matching Evidence page, add as many of the evidence files to the case as you want. By default, all evidence is selected.

    - If you want to add evidence to the case, ensure that the check box to the left of the evidence is selected and then click **Add to Case**.

      If more than 40 evidence files match the case ID, you can add 40 at a time and click **Continue** to see the next set of files.

    - If you want to go to the case without adding some or any of the evidence found, click **Skip to Case**.

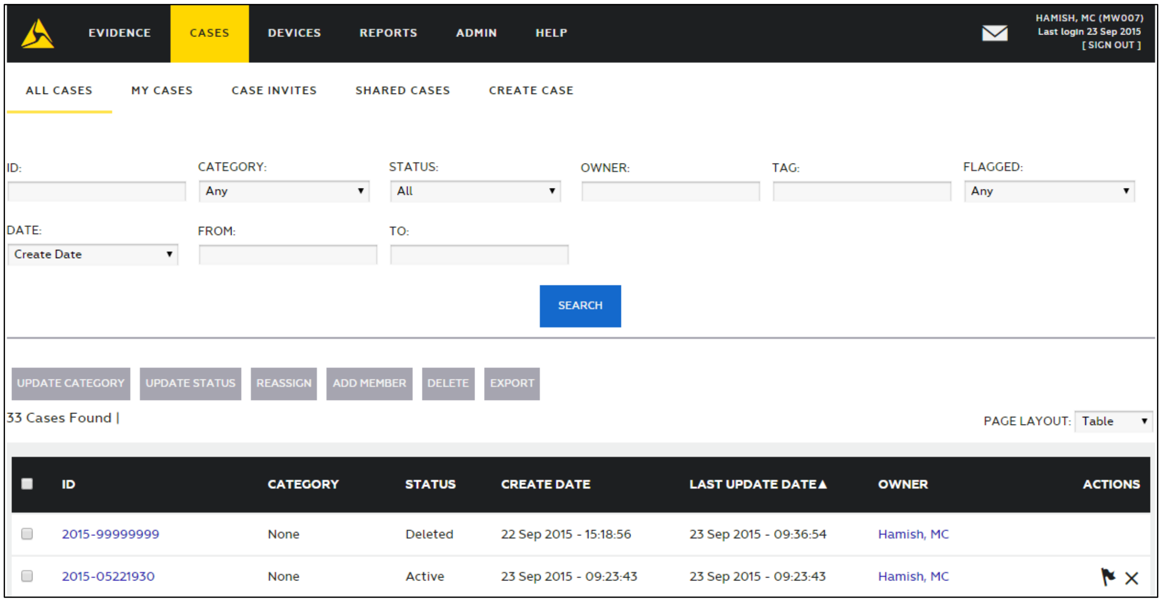
    When you are finished adding evidence, Evidence.com displays the View Case page.

5. Use the case as needed. For more information about available actions, see Working with Cases.

Case Search — All Cases, My Cases, and Shared Cases

Evidence.com provides case search features to help you find the cases that you need. In the Cases area, you can use any of the three case-search pages:

- **All Cases**—Finds all cases, including cases you may not have permission to view.
- **My Cases**—Finds cases that you own. The Owner filter is automatically set to your name.
- **Shared Cases**—Finds cases that have been shared with you by the case owner or another user with permission to share the case.



ID:
CATEGORY: Any
STATUS: All
OWNER:
TAG:
FLAGGED: Any
DATE: Create Date
FROM:
TO:

33 Cases Found |

PAGE LAYOUT: Table

■	ID	CATEGORY	STATUS	CREATE DATE	LAST UPDATE DATE▲	OWNER	ACTIONS
□	2015-99999999	None	Deleted	22 Sep 2015 - 15:18:56	23 Sep 2015 - 09:36:54	Hamish, MC	
□	2015-05221930	None	Active	23 Sep 2015 - 09:23:43	23 Sep 2015 - 09:23:43	Hamish, MC	⚑ ✕

1. On the menu bar, click **Cases**.

   The All Cases page lists all cases, sorted by the date they were last updated.

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

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	1. Update the case search filters. For more information, see Case Search Filters. 2. Click **Search**.
Sort search results	Click the column heading for **ID**, **Create Date**, or **Last Update Date**. To reverse the sort order, click the heading again.
Switch between page layout options (table or detailed)	On the **Page Layout** list, click the layout you want.

For information about the actions you can take from search results, see Working with Case Search Results.

Case Search Filters

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

- **ID** — Limits search results to cases whose ID includes the characters you enter in the ID box. For more information, see Text Search Details.
- **Category** — Limits search results to cases that are assigned to the category that you select. By default, search results include cases assigned to any category, including uncategorized cases.
- **Status** — Limits search results to cases whose status matches the status selected. By default, case searches include all statuses.
- **Owner** — Limits search results to cases owned by the user specified. To specify the user, click in the Owner box, start typing the name of the user, wait for Evidence.com to show the matching users, and then click the user you want.

  On the My Cases page, the Owner filter is set to your name by default.

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

- **Flagged** — Limits search results to cases whose flag status matches the flag status selected.

- **Date** — Limits search results by either the creation date of the case or the last date that the case was updated, as selected. You must also specify a date range by using the From and To boxes; otherwise, the search is not limited by date range. Search results are inclusive of the dates specified.

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

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

Text Search Details

For case searches, the ID and Tag filters provide advanced text matching features.

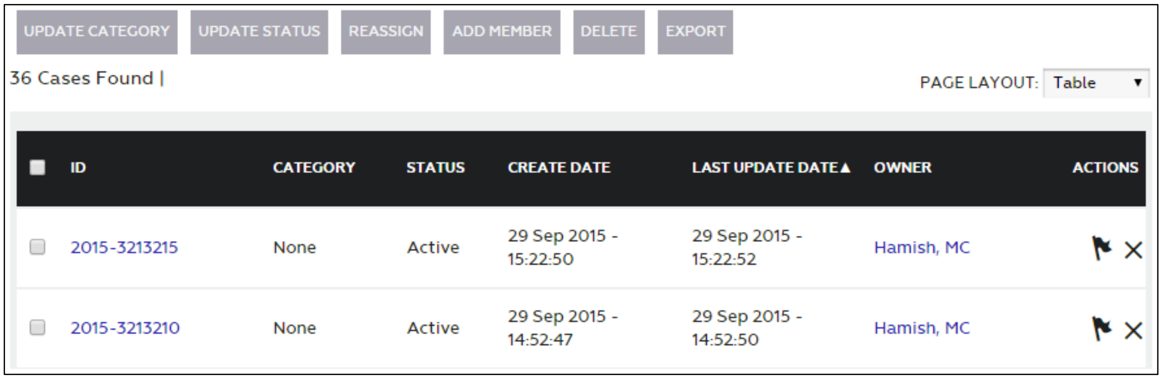
- The text you enter can match any part of the data you are filtering. For example, if you enter `2112` in the ID box, any case whose ID includes “2112” in any portion of the ID is included in search results.

- You can search for more than one text string in a single filter. For example, if you enter `21 78` in the ID box, search results include evidence with the ID 213789 as well as 421278.

- The order of text strings is irrelevant. For example, if you enter `78 21` in the ID box, search results include cases with the ID 213789.

Working with Case Search Results

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



36 Cases Found |

PAGE LAYOUT: Table ▾

■	ID	CATEGORY	STATUS	CREATE DATE	LAST UPDATE DATE▲	OWNER	ACTIONS
□	2015-3213215	None	Active	29 Sep 2015 - 15:22:50	29 Sep 2015 - 15:22:52	Hamish, MC	⚑ ×
□	2015-3213210	None	Active	29 Sep 2015 - 14:52:47	29 Sep 2015 - 14:52:50	Hamish, MC	⚑ ×

View Case

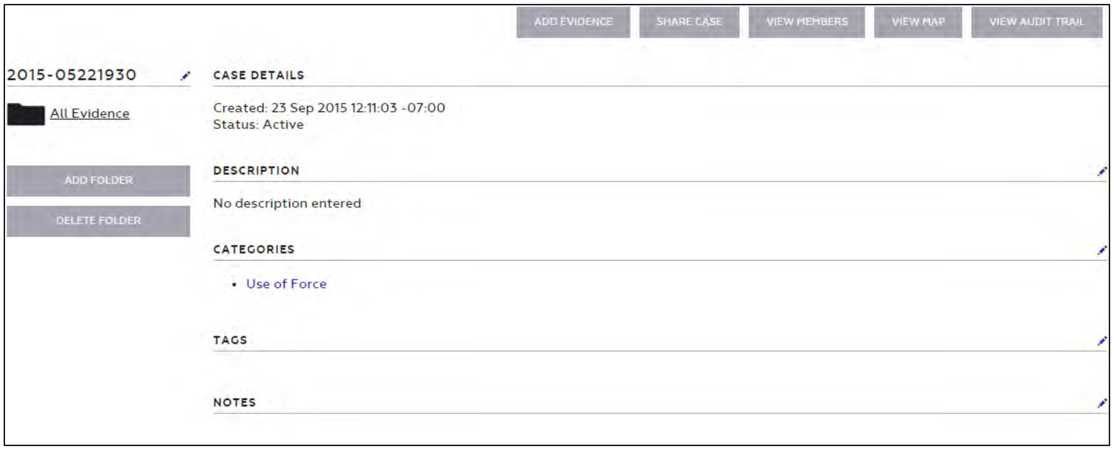
You can view cases listed in case search results if any of the following are true:

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

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

   The View Case page opens.

For information about the actions you can take from the View Case page, see Working with Cases.



2015-05221930

All Evidence

CASE DETAILS

Created: 23 Sep 2015 12:11:03 -07:00
Status: Active

DESCRIPTION

No description entered

CATEGORIES

- Use of Force

TAGS

NOTES

Add a Category to Cases

You can add a category to one or more cases in search results.

1. Search for the cases that you want to add a category to.
2. For each case that you want to add a category to, select the check box to the left of the case.
3. Above the search results, click **Update Category**.

   A dialog box appears.
4. In the New Category list, click the category that you want to add to all selected cases and then click **Update**.
5. On the notification message box, click **OK**.

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

Update the Status of Cases

You can change the status assigned to one or more cases in search results. If you want to change the status of a case to Deleted, see Delete Case.

1. Search for the cases whose status you want to update.
2. For each case whose status you want to update, select the check box to the left of the case.

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

   A dialog box appears.

4. In the Status list, click the status that you want to assign to all selected cases and then click **Update**.

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

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

Delete Cases

You can delete cases that are listed in case search results. Deleting a case changes the status of the case being Deleted.

Note: When you delete a case, Evidence.com removes all evidence from the case and Evidence.com begins enforcing the retention policy determined by the categories assigned to the evidence. This may result in evidence being immediately queued for deletion.

1. Search for the cases that you want to delete.

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

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

   A confirmation dialog box appears.

4. Click **OK**.

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

6. If you want to confirm that the case status is Deleted, click **Search**, locate the case in the search results, and view the case status.

Reassign Cases

When you need to change the owner of a case to another user or to a group, you can reassign the cases from the results of a case search.

If you reassign a case to a group, Evidence.com chooses one user from the group to be the case owner. Evidence.com assigns the other users to the case as members. When it chooses an owner, Evidence.com prioritizes the choice.

1. Group monitor — If the group has monitors, Evidence.com chooses the owner from the monitors of the groups, choosing at random if there is more than one monitor to choose from.
2. Group member — If the group has no monitors, Evidence.com chooses the owner from among the members of the group, choosing at random if there is more than one member to choose from.

1. Search for the cases that you want to reassign to another user.
2. For each case that you want to reassign, select the check box to the left of the case.
3. Above the search results, click **Reassign**.

   A dialog box appears.
4. In the **Reassign To** box, start typing the name of the user or group to whom you want to assign the cases, wait for Evidence.com to show the list of matching users and groups, click the user or group that you want, and then click **Reassign**.
5. In the confirmation dialog box, click **OK**.

   The search results show that the user or group who you selected is now the case owner.

Add a Member to Cases

When you need to share a case with users who are in your agency, you can add users to cases from the results of a case search.

If you want to share a case with people in a partner agency, see Share a Case with a Partner Agency.

1. Search for the cases that you want to share.
2. For each case that you want to share, select the check box to the left of the case.

3. Above the search results, click **Add Member**.

   A dialog box appears.

4. In the **Enter User** box, start typing the name of the user you want to share with, wait for Evidence.com to show the list of matching users, click the user that you want, and then click **Share**.

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

Export Case Search Results

You can export the results of a case search in PDF, Microsoft Excel, text, or CSV format.

If the search results contain more than 500 cases, Evidence.com exports the search results in 500-case segments and asks you to confirm the download of the next segment.

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

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

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

   The case search results download in the format that you specified.

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

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

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

Flag and Un-flag Cases

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

On any case search page, each case in the search results has a Flag or Unflag button in the Actions column.

- Cases that are *not* flagged have a black ⚑ (flag) button.
- Cases that are flagged have a red ⚑ (unflag) button.

If you want to flag or un-flag a case, click ⚑ (flag) or ⚑ (unflag), as applicable.

Working with Cases

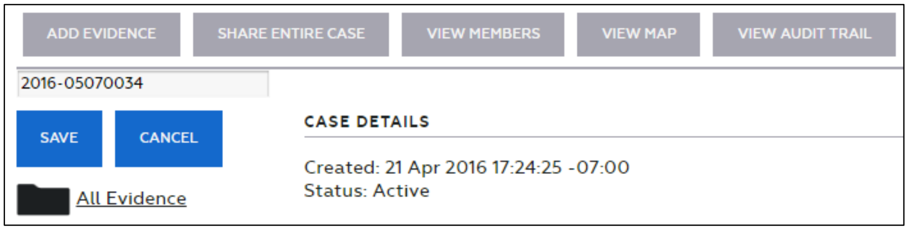
This section describes the actions available on the View Case page for any case.

Edit Case ID

On the View Case page, the case ID appears in the upper-left corner.

1. To the right of the case ID, click ✎ (edit).

   The case ID becomes editable.



2016-05070034

CASE DETAILS

Created: 21 Apr 2016 17:24:25 -07:00
Status: Active

2. Change the case ID, as needed, and then click **Save**.

   The View Case page shows the updated ID.

Edit the Description of a Case

You can add or edit a description of the case.

On the View Case page, the description appears below the case.

1. To the left of **Description**, click ✎ (edit).

   The description text becomes editable.

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

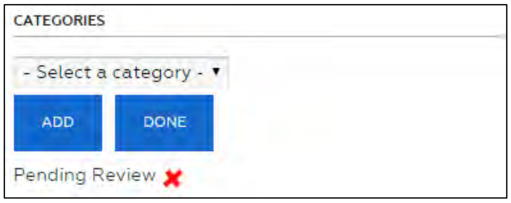
   Evidence.com saves the case description changes.

Assign and Unassign Categories

On the View Case page, the Categories area appears below the case description. The Categories area lists the categories that the case is assigned to, if any.

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

   The “Select a category” list appears. If the case is already assigned to categories, a red **X** appears beside each assigned category.

   Pending Review ✖

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

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

3. If you want to remove the case from a category, click the red **X** next to the category and then, on the confirmation message box, click **OK**.

   Evidence.com removes the category from the list of assigned categories.

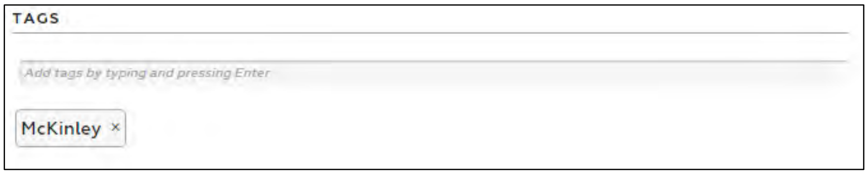
4. When you are finished editing category assignments, click **Done**.

Add and Remove Tags for Cases

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

Tags are labels that you can apply to cases. You can add tags to cases that you want to find more easily in the future. Case searches allow you to filter the search results by tags.

On the View Case page, the Tags area appears below the description and the Categories area. If any tags exist, they appear as tiles. The following figure shows an example of the Tags area that has one tag named, “McKinley”.



McKinley ×

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

Notes and Cases

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

On the View Case page, the Notes area appears below the description, the Categories, and the Tags areas.

Add a Note

You can post a note to a case.

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

2. To the right of **Notes**, click ✎ (edit).

   An editable box appears in the Notes area.

3. In the box, type the note and then click **Add Note**.

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

Edit a Note

You can edit notes that have previously been posted to a case.

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

2. To the right of the note, click **Edit**.

   The note text becomes editable.

3. Edit the note text as needed.

4. Click **Update**.

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

Delete a Note

You can delete notes that you have posted.

1. If necessary, scroll down and find the Notes area.
2. To the right of the note, click **Delete**.
3. On the confirmation dialog box, click **OK**.

   The note no longer appears on the View Case page.

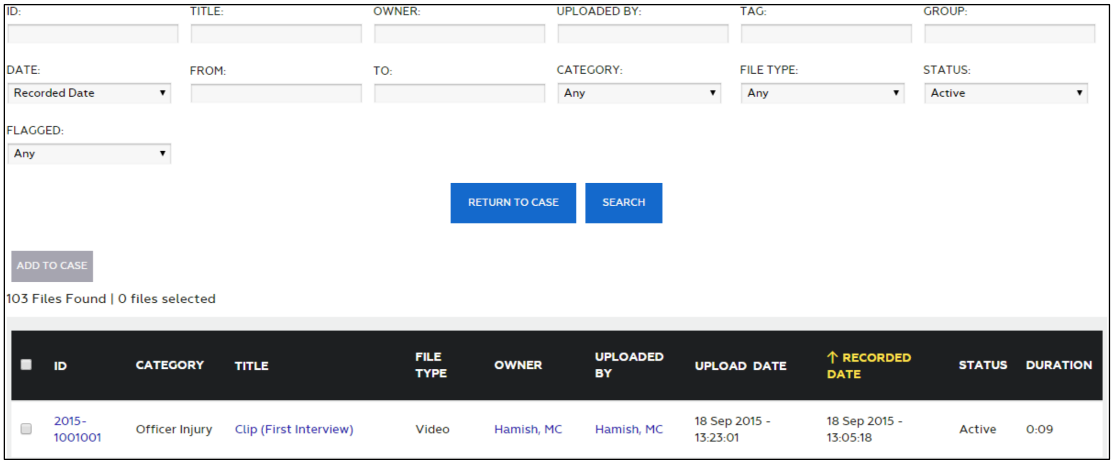
Add Evidence to a Case

From the View Case page, you can add evidence to the case you are viewing; however, you cannot add evidence to a case whose status is Deleted.

If a case is shared with partner agencies and you add evidence to the case, Evidence.com provides you the option of sharing the additional evidence with the partner agencies.

1. Above the Case Details area, click **Add Evidence**.

   An evidence search page appears.



ID:
TITLE:
OWNER:
UPLOADED BY:
TAG:
GROUP:
DATE: Recorded Date ▾
FROM:
TO:
CATEGORY: Any ▾
FILE TYPE: Any ▾
STATUS: Active ▾
FLAGGED: Any ▾

103 Files Found | 0 files selected

□	ID	CATEGORY	TITLE	FILE TYPE	OWNER	UPLOADED BY	UPLOAD DATE	↑ RECORDED DATE	STATUS	DURATION
□	2015-1001001	Officer Injury	Clip (First Interview)	Video	Hamish, MC	Hamish, MC	18 Sep 2015 - 13:23:01	18 Sep 2015 - 13:05:18	Active	0:09

2. Search for the evidence that you want to add to the case.

   If you need to refine the search results, use the search filters as needed. For more information, see Evidence Search Filters.

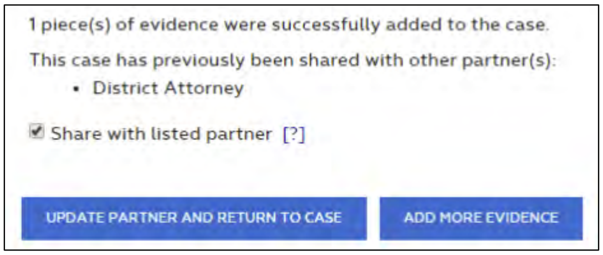
3. For each evidence file that you want to add to the case, select the check box to the left of the evidence ID.

4. Click **Add to Case**.

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

   A dialog box provides you the choice of continuing to add evidence or returning to the case.

   If the case is shared with partner agencies, the dialog box also includes the option to share the additional evidence with all the partner agencies with whom the case is shared.



1 piece(s) of evidence were successfully added to the case.

This case has previously been shared with other partner(s):

- District Attorney

☑ Share with listed partner [?]

6. If you want to continue adding evidence, click **Add More Evidence** and then return to step 2.

7. If you have finished adding evidence, do one of the following actions:

   - If the dialog box does not list partner agencies, click **Return to Case**.
   - If you want to share the additional evidence with the listed partner agencies, ensure that the **Share with listed partner check box** is selected, and then click **Update Partner and Return to Case**.
   - If you *do not* want to share the additional evidence with the listed partner agencies, clear the **Share with listed partner check box**, and then click **Return to Case**.

   The View Case page reappears.

   If you chose to share the additional evidence with partner agencies, Evidence.com notifies them that there is additional evidence.

8. If you want to confirm that the evidence was added to the case, click **All Evidence** and view the list of evidence files assigned to the case.

Remove Evidence from a Case

From the View Case page, you can remove evidence from the case you are viewing.

Note: If the case and the evidence you are removing is shared with partner agencies, removing the evidence from the case in your agency has no effect on the copy of the case in partner agencies.

1. On the View Case page, click an evidence folder that the evidence is in.

   Below the evidence preview area, a list of evidence in the case appears.

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

3. Above the evidence list, click **Remove from Case**.

4. On the confirmation dialog box, click **Remove**.

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

   Evidence.com removes the evidence from the case. The evidence list updates to reflect the removal of the evidence.

Work with Evidence Folders

Evidence folders provide you a way to organize evidence files. After you add evidence to a case, you can add the evidence to as many folders as you need. For example, you could create a folder for all evidence files in the case that prove a particular fact.

The All Evidence folder always includes all evidence in a case. You cannot delete the All Evidence folder.

You can add as many folders as you need; however, after you add folder, you cannot rename it. Instead of renaming a folder, you can create a new folder, add the evidence from the old folder to the new folder, and then remove the old folder.

Add a Folder

1. On the View Case page, below the case ID, click **Add Folder**.

2. On the dialog box, in the **Enter Folder Name** box, type a meaningful name for the folder, and then click **Add**.

   Evidence.com creates the folder and adds it to the list of folders below the case ID.

Delete a Folder

You can delete any folder that you created. You cannot delete the All Evidence folder.

1. On the View Case page, below the case ID, click **Delete Folder**.
2. On the dialog box, in the **Select Folder** list, click the folder that you want to remove, and then click **Delete**.
3. On the notification message box, click **OK**.

Add Evidence to a Folder

For evidence that is already in a case, you can add the evidence to any evidence folder that you need.

If you need to add evidence to the case, see Add Evidence to a Case.

1. On the View Case page, click an evidence folder that the evidence is already in.

   Note: You can always use the All Evidence folder for this purpose.

   Below the evidence preview area, a list of evidence in the folder appears.
2. In the list, for each evidence file that you want to add to another folder, select the check box to the left of the evidence title.
3. Above the evidence list, click **Add to Folder**.
4. On the dialog box, in the **Select Folder** list, click the folder you that you want to add the evidence to, and then click **Select**.
5. On the confirmation message box, click **OK**.

   Evidence.com adds the evidence to the folder that you selected.
6. If you want to confirm that the evidence is in the folder that you added to, below the case ID, click the folder and view the evidence list.

Remove Evidence from a Folder

You can remove evidence from any evidence folder, as needed. The exception is the All Evidence folder; you can never remove evidence from the All Evidence folder.

If you need to remove evidence from a case, see Remove Evidence from a Case.

1. On the View Case page, click the evidence folder from which you want to remove evidence.

Below the evidence preview area, a list of evidence in the folder appears.

2. In the list, for each evidence file that you want to remove from the folder, select the check box to the left of the evidence title.

3. Above the evidence list, click **Remove from Folder**.

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

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

   Evidence.com removes the selected evidence from the folder. The evidence remains in the case.

Work with Evidence in a Case

For evidence that is in a case, you can perform the actions described in this section.

Preview Evidence in a Case

From the View Case page, you can view evidence that is in the case. Preview is only available for some of the supported evidence file types.

1. On the View Case page, click an evidence folder that the evidence is in.

   Below the evidence preview area, a list of evidence in the case appears.

2. In the list, find the evidence that you want to preview and then click 🔍.

   If the evidence file type is supported, the preview area shows the evidence file.

View Evidence from a Case

From a View Case page, you can open the View Evidence page for evidence included in the case.

1. On the View Case page, click an evidence folder that the evidence is in.

   Below the evidence preview area, a list of evidence in the case appears.

2. In the list, find the evidence that you want to view and then click the evidence title.

   The View Evidence page appears. For more information, see Working with Any Evidence.

Download Evidence from a Case

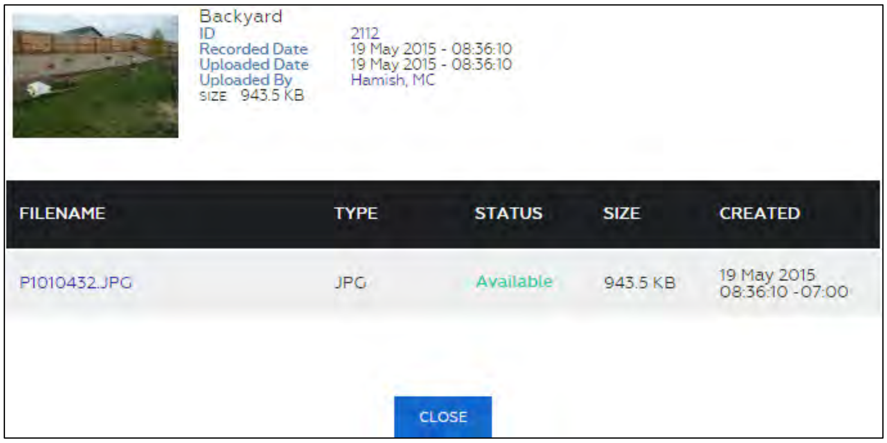
From a View Case page, you can download evidence files for evidence included in the case.

1. On the View Case page, click an evidence folder that the evidence is in.

   Below the evidence preview area, a list of evidence in the case appears.

2. In the list, find the evidence that you want to download and then click ⤓.

   A dialog box shows information about the evidence file.



Backyard

ID	2112
Recorded Date	19 May 2015 - 08:36:10
Uploaded Date	19 May 2015 - 08:36:10
Uploaded By	Hamish, MC
SIZE 943.5 KB	

FILENAME	TYPE	STATUS	SIZE	CREATED
P1010432.JPG	JPG	Available	943.5 KB	19 May 2015 08:36:10 -07:00

3. Under **Filename**, click the evidence file name.

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

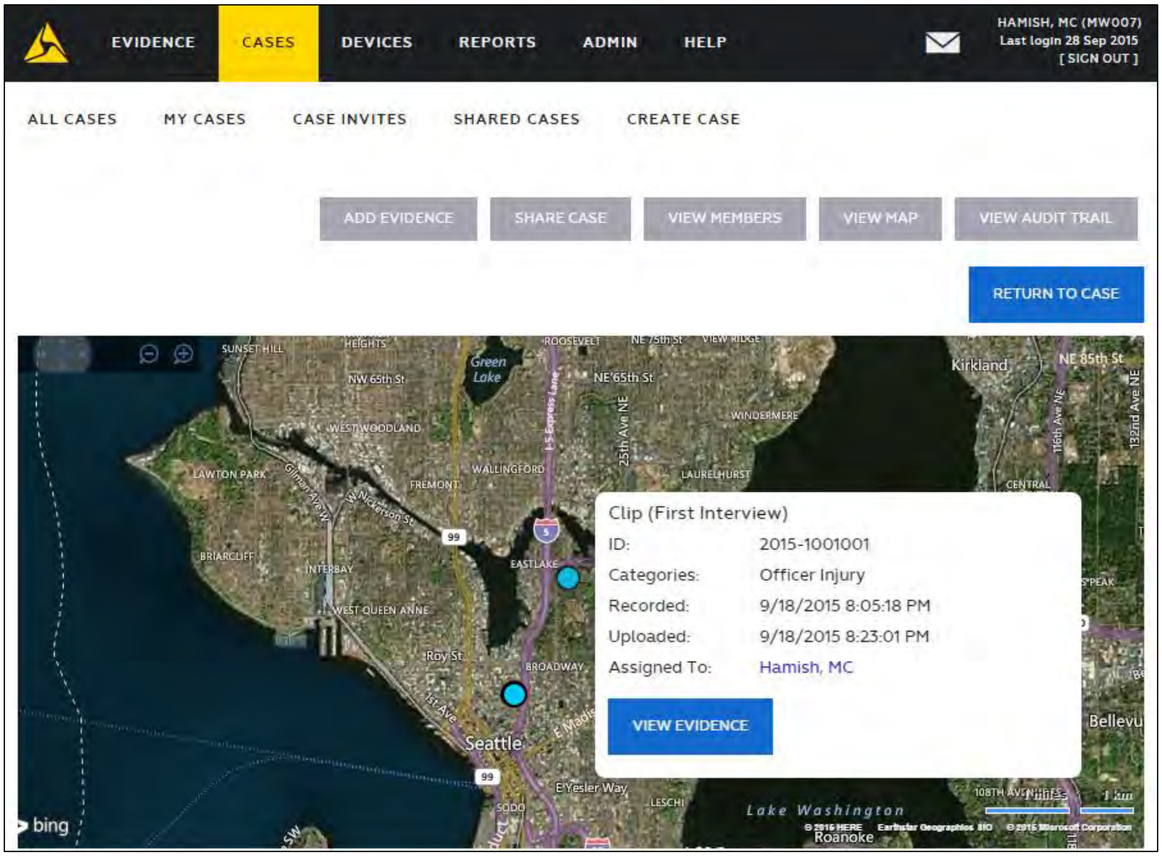
4. Click **Close**.

View Map

You can view an evidence map that shows the location of evidence in the case, if the evidence has location information. For more information, see Edit Location.

The map pin style used for an evidence file is determined by the retention category assigned to the evidence.

To view an evidence map of a case, on the View Case page, click **View Map**.



Clip (First Interview)

ID:	2015-1001001
Categories:	Officer Injury
Recorded:	9/18/2015 8:05:18 PM
Uploaded:	9/18/2015 8:23:01 PM
Assigned To:	Hamish, MC

Case Evidence Map Actions

A case evidence map provides basic features for finding and viewing a 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	1. Hover the mouse pointer over the pin 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 View Evidence page opens.
Pan	At the left end of the map tool bar, click the directional pad in the direction that you want to pan the map. Alternately, do the following steps: 1. Position the mouse pointer over the map. 2. Click and hold the mouse button. 3. Move the mouse to pan the map.
Zoom In or Zoom Out	1. In the map tool bar, hover the mouse pointer over the magnifying glass icons. 2. Use the slider to zoom in or out. Alternately, if your mouse has a mouse wheel: 1. Position the mouse pointer over the map. 2. Rotate the mouse wheel to zoom in or out.

View Case Audit Trail

You can view the audit trail for a case. On the View Case page, the View Audit Trail button appears in the upper-right corner of the page.

1. Click **View Audit Trail**.

   A dialog box shows options for viewing the entire audit trail or a portion of the audit trail.

2. If you want to view the whole audit trail, under **View entire audit log**, click **Submit**.

3. If you want to view a portion of the audit trail, under **View portion of audit log**, specify a date in either or both the **From** or **To** boxes and click **Submit**.

   Evidence.com opens or downloads a PDF for the case audit trail. The exact behavior depends on the browser you use and its download settings for PDF files.

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

Sharing Cases Inside and Outside Your Agency

Evidence.com provides three ways to share cases, each allowed or prohibited by a separate permission, enabling administrators to control sharing closely.

Share a Case with Other Users in Your Agency

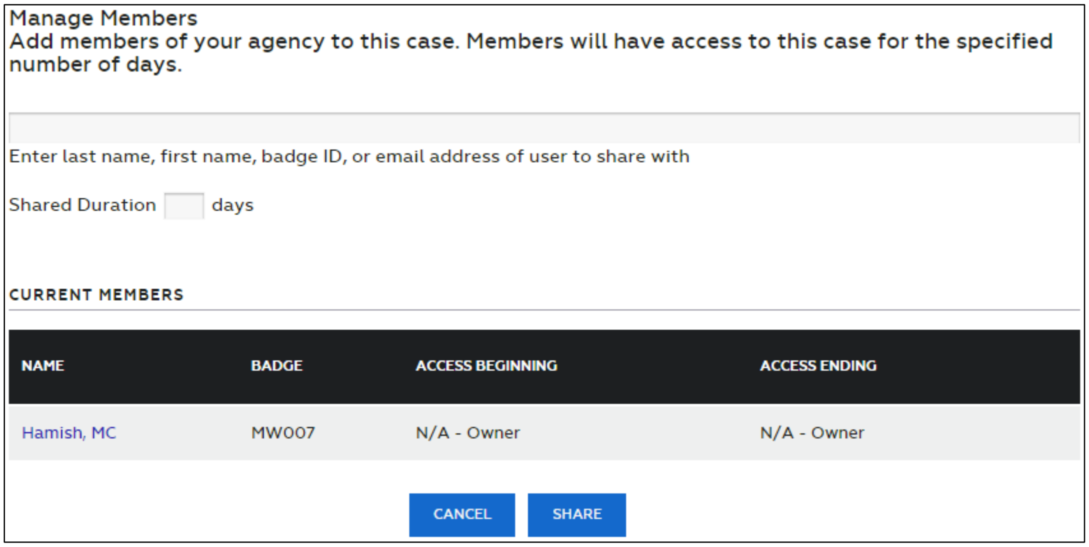
Administrators and users allowed the Case Management “Share” permission can share cases with other users in your agency. Users who you share a case with are *members* of the case. Case members can only access the case after signing in to your Evidence.com agency.

1. Search for the case that you want to share.
2. In the list of cases, find the case that you want to share and then click the ID of the case.

   The View Case page appears.
3. Click **Share Entire Case**.

   A dialog box presents the three case sharing options.
4. Click **Add Agency Members** and then click **Next**.

   The Manage Members dialog box appears.



Manage Members

Add members of your agency to this case. Members will have access to this case for the specified number of days.

Enter last name, first name, badge ID, or email address of user to share with

Shared Duration days

CURRENT MEMBERS

NAME	BADGE	ACCESS BEGINNING	ACCESS ENDING
Hamish, MC	MW007	N/A - Owner	N/A - Owner

5. For each user who you want to share the case with, start typing the name of the user, wait for Evidence.com to show the matching users, and then click the user you want. You can also type the user badge ID or email address.

   Each user you select appears above the box.

6. In the **Shared Duration** box, enter the number of days that the evidence is to be available to the users you are sharing the case with.

7. When you have finished adding all the users with whom you want to share this case, click **Share**.

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

   Evidence.com sends each user an email that invites them to share the case.

Share a Case by Download Link

Sharing by download link enables you to share a case and its evidence with anyone who uses the download link during the sharing duration. A download link is a web link that allows anyone with the link and a web browser to access the case and its evidence. This method of sharing is unauthenticated, that is, downloading the case and its evidence does not require signing in to an Evidence.com agency.

Note: It is recommended that, whenever possible, you share cases and evidence using an authenticated sharing method, such as sharing with users in your agency and sharing with partner agencies. This ensures that only the people you intend to grant access to a case and its evidence do receive access.

If you need to share a case with someone who is not a user in your agency or a partner agency, consider using the bulk evidence-sharing feature, which supports sharing with users of my.evidence.com. Anyone with access to email can create an account on my.evidence.com. Evidence you share with a my.evidence.com account is only available to people who know the user credentials for authenticated access to the account. For more information, see Bulk Share Evidence by Authenticated Sharing.

Evidence.com supports the following file types for the case download file:

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

Administrators and users allowed the Case Management “Share External Download Links” permission can share cases by download link.

1. Search for the case that you want to share.

2. In the list of cases, find the case that you want to share and then click the ID of the case.

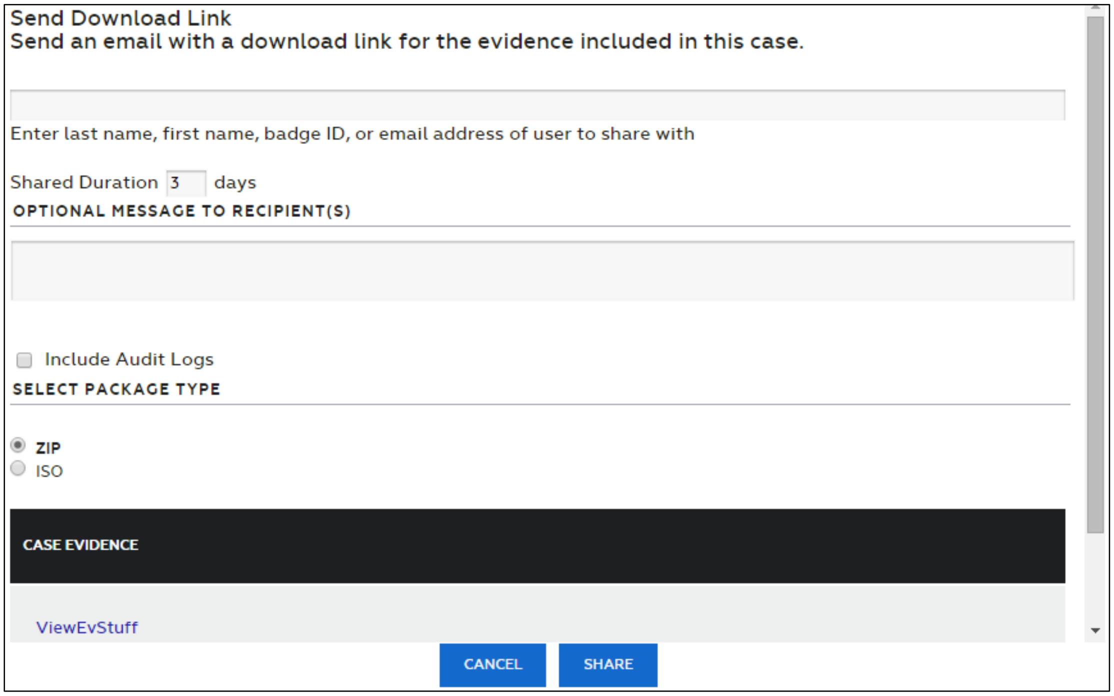
   The View Case page appears.

3. Click **Share Entire Case**.

   A dialog box presents the three case sharing options.

4. Click **Send Download Link** and then click **Next**.

   The Send Download Link dialog box appears.



Send Download Link
Send an email with a download link for the evidence included in this case.

Enter last name, first name, badge ID, or email address of user to share with

Shared Duration 3 days

OPTIONAL MESSAGE TO RECIPIENT(S)

□ Include Audit Logs

SELECT PACKAGE TYPE

● ZIP
○ ISO

CASE EVIDENCE

ViewEvStuff

5. Use the first box to add the people with whom you want to share the case and its evidence, as follows:

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

     The user you selected appears above the box. If the user is in your agency, the user has a white background. If the user is in a partner agency, the user has a green background.

   - For a person who is not a user in your agency or in a partner agency, type the email address of the person and then press **Enter**.

     If the person already has a my.evidence.com account, the email address appears above the box, with a yellow background.

     If the person does not have a my.evidence.com account, the email address remains in the first box. The person receives an email with the download link; however, if you need to add more users, complete this procedure, and then repeat it until you have shared the evidence with all required users.

6. In the **Shared Duration** box, type the number of days that the case is to be available for download.
7. If you want to include audit logs, check the corresponding check box.
8. Under **Select Package Type**, select the file type that you want for the download file.
9. Click **Share**.
10. On the notification message box, click **OK**.

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

    Evidence.com makes the case and its evidence available for download, until the sharing duration expires.

Share a Case with a Partner Agency

Evidence.com makes it easy to share cases and their evidence to organizations such as City and District Attorneys. After you have added the evidence, you share the case with the trusted partner agencies that you choose.

Administrators and users allowed the Case Management “Share with Partner Agencies” permission can share cases with partner agencies.

When you share a case with a partner agency, Evidence.com sends the partner agency a *copy* of the files, which they can manage independently, with no effect on your case and its evidence.

Note: If you want to allow users in a partner agency to have only temporary access to evidence, consider bulk sharing the evidence rather than sharing the case. For more information, see Bulk Share Evidence by Authenticated Sharing.

Evidence.com copies the metadata applied to the case, too. For more information, see Receiving Shared Cases from Partner Agencies.

After Evidence.com finishes copying the case to receiving agencies, Evidence.com notifies the recipients that the shared case is available. Recipients can begin managing the case as needed.

1. Search for the case that you want to share.
2. In the list of cases, find the case that you want to share and then click the ID of the case.

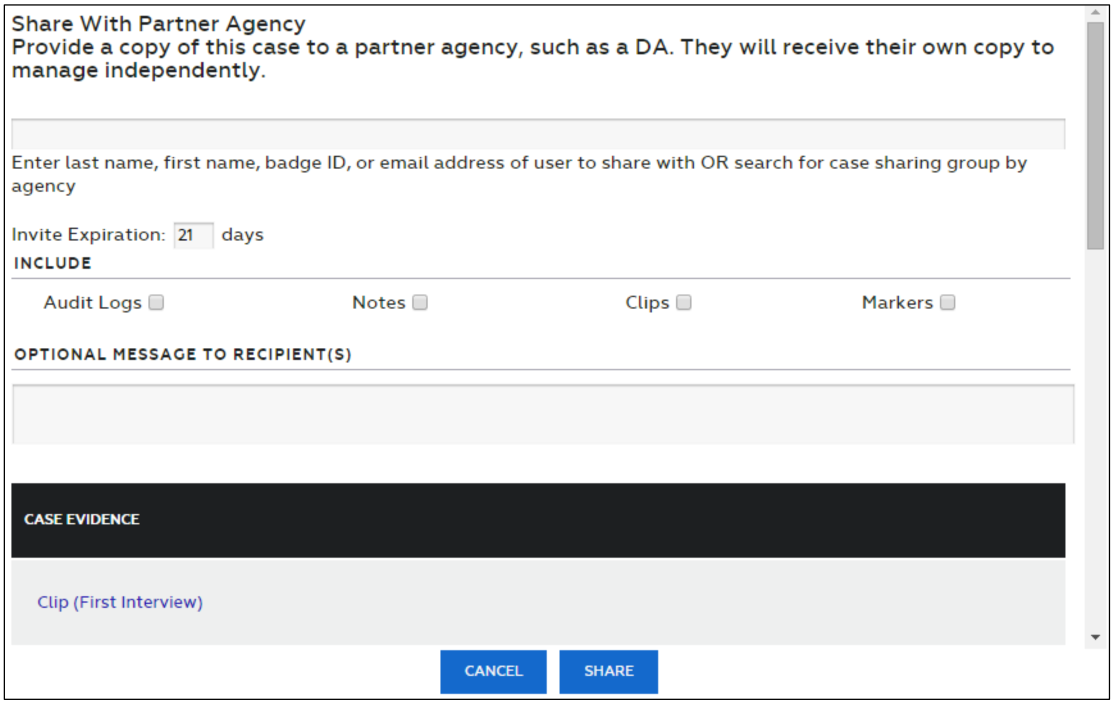
The View Case page appears.

3. Click **Share Entire Case**.

   A dialog box presents the three case sharing options.

4. Click **Share With Partner Agency** and then click **Next**.

   The Share with Partner Agency dialog box appears.



Share With Partner Agency
Provide a copy of this case to a partner agency, such as a DA. They will receive their own copy to manage independently.

Enter last name, first name, badge ID, or email address of user to share with OR search for case sharing group by agency

Invite Expiration: 21 days

INCLUDE

Audit Logs □ Notes □ Clips □ Markers □

OPTIONAL MESSAGE TO RECIPIENT(S)

CASE EVIDENCE

Clip (First Interview)

5. Use the first box to add the users or groups of the partner agency with whom you want to share the case, as follows:

   - To share with a *user* in a partner agency, start typing the name of the *user*, wait for Evidence.com to show the matching users, and then click the user you want. You can also type the user badge ID or email address.

     The user you selected appears above the box.

   - To share with a *group* in a partner agency, start typing the name of the *agency*, wait for Evidence.com to show the available groups of matching agencies, and then click the group you want.

     The group you selected appears above the box.

If you add the wrong user or group, you can remove it by clicking the ✕ at the right end of the user or group name.

6. In the **Invite Expiration** box, type the number of days that the invitation to share the case is valid.

7. Under **Include**, select the check boxes for the additional information that you want to give to the partner agencies you are sharing with.

8. In the **Optional Message to Recipient(s)** box, type any useful or required message, as needed.

9. If you want to review the evidence that you are sharing, under **Case Evidence**, view the evidence list. Scroll down as needed. If you want to view evidence in a new browser window, click the evidence title.

10. Click **Share** and then, on the confirmation message box, click **OK**.

    Evidence.com copies to the partner agency the case, its evidence, and any of the additional information you included. After the copy is complete, Evidence.com emails the users and group members with whom you shared the case, notifying them that the shared case is available.

Update Partner Agency When Adding Evidence

When you add evidence to a case that you have shared with a partner agency, Evidence.com prompts you to update the partner agencies. If the Share with listed Partner(s) check box is selected, Evidence.com send invites to all of the agencies you have previously shared with to accept the newly added evidence.

For more information, see Add Evidence to a Case.

Update Partner Agencies from the Case Members Page

The Partners list, available on the View Case page after you click View Members, displays the partner agencies that the case is shared with, including whether each partner agency's copy of the case is up to date.

If a partner agency status is “Out of Date”, the partner agency's copy of the case is missing evidence. You can share the evidence that the partner agency is missing by selecting Update.

For more information, see View, Update, Add, and Remove Members.

View, Update, Add, and Remove Members

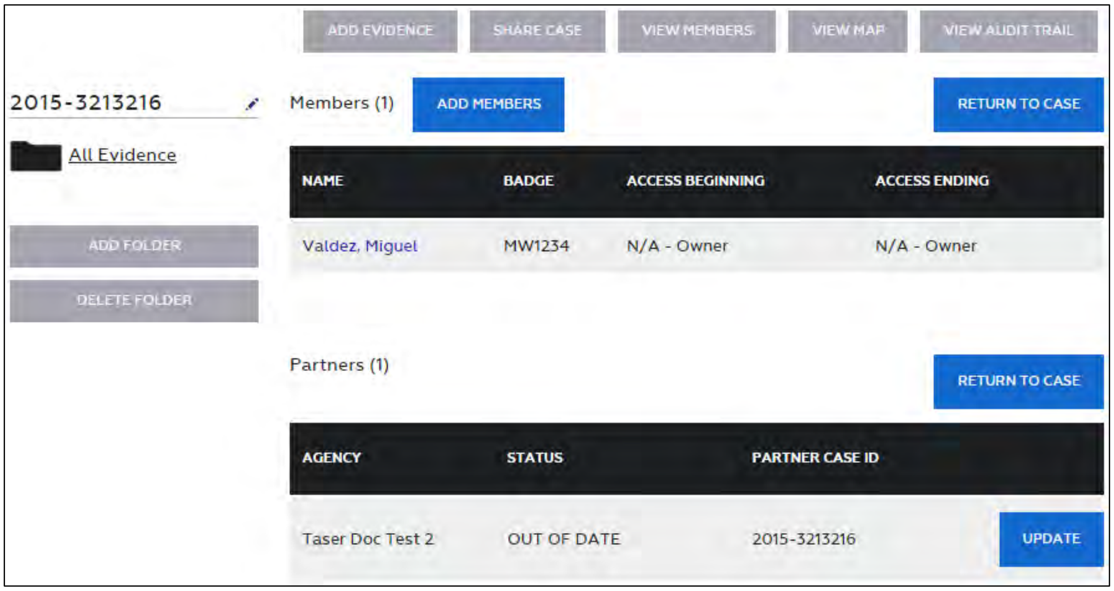
When you want to know who has access to a case, you can view lists of users and partner agencies with whom the case is shared.

Case members are the users who have access to the case, including the case owner. Additionally, partner agencies with whom a case is shared are also considered members.

1. On the View Case page, click **View Members**.

   Evidence.com shows a list of users in your agency who have access to the case. The case owner is listed first. Users with whom the case is shared are listed below the owner.

   If the case is shared with partner agencies, they are listed below the list of users.



NAME	BADGE	ACCESS BEGINNING	ACCESS ENDING
Valdez, Miguel	MW1234	N/A - Owner	N/A - Owner

AGENCY	STATUS	PARTNER CASE ID
Taser Doc Test 2	OUT OF DATE	2015-3213216

2. Take any additional actions that you need. The following table provides information about the available actions.

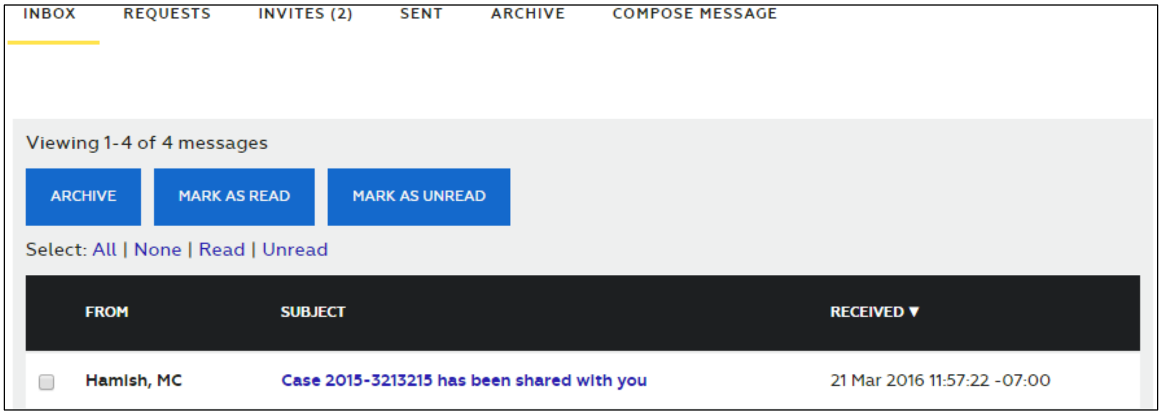
Action	Steps
Add a user	**Note:** It is recommended that you add members to a case by following the steps in Share a Case with Other Users in Your Agency. 1. Above the list of users, click **Add Member**. A user search page appears. 2. Search for the user you want to add to the case. 3. To the left of the user name, select the check box. 4. Above the search results, click **Add to Case**. 5. In the **Length (In Days) to Share This Case** box, type the number of days that the user should have access to the case, and then click **OK**. 6. On confirmation message box, click **Return to Case**.

Action	Steps
Add a partner agency	Perform the steps in Share a Case with a Partner Agency. You cannot add a partner agency from the list of case members.
Update a partner agency	1. Under **Partners**, find the agency whose status is "Out of Date". 2. To the right of the partner agency name, click **Update**. 3. On the notification message box, click **OK**. The status of the partner agency changes to "Awaiting Acceptance". Evidence.com sends the partner agency an invitation to accept the additional evidence.
View user information	1. Find the user in the list of case members. 2. Click the user name. The User Summary page appears.
Remove a user from the case	1. Find the user in the list of case members. 2. To the right of the user name, click ✕ (remove member). 3. On the confirmation message box, click **Yes**. 4. On the notification message box, click **OK**.

Receiving Shared Cases from Partner Agencies

When a partner agency shares a case with users or groups in your agency, Evidence.com copies the case to your agency first and then sends a notification message to each recipient. No approval or acceptance of the case is required. Because cases shared from a partner agency are a *copy* of the files, you can manage the case and its evidence independently, with no effect on the case or evidence in the partner agency.

Your agency can manage the case as you would a case that was created in your agency. When Evidence.com copies the case to your agency, assumptions are made regarding case ownership, metadata, and audit logs, as described in the following sections.



Viewing 1-4 of 4 messages

Select: All | None | Read | Unread

FROM	SUBJECT	RECEIVED ▼
□ Hamish, MC	Case 2015-3213215 has been shared with you	21 Mar 2016 11:57:22 -07:00

Assignment of Case Ownership

Cases can have only one owner; however, a partner agency can specify more than one user or group in your agency to share a case with. Evidence.com chooses one user to be the case owner. Evidence.com assigns the other users to the case as members.

When it chooses an owner, Evidence.com prioritizes the choice.

1. Users — If the case is shared with more than one user or a user and groups, Evidence.com chooses the owner from the users, choosing at random if there is more than one individual user to choose from.
2. Group monitor — If the case is shared with one or more groups but no individual users, Evidence.com chooses the owner from the monitors of the groups, choosing at random if there is more than one monitor to choose from.
3. Group member — If the case is shared with one or more groups that have no monitors and is not shared with individual users, Evidence.com chooses the owner from among the members of the groups, choosing at random if there is more than one member to choose from.

Case Metadata

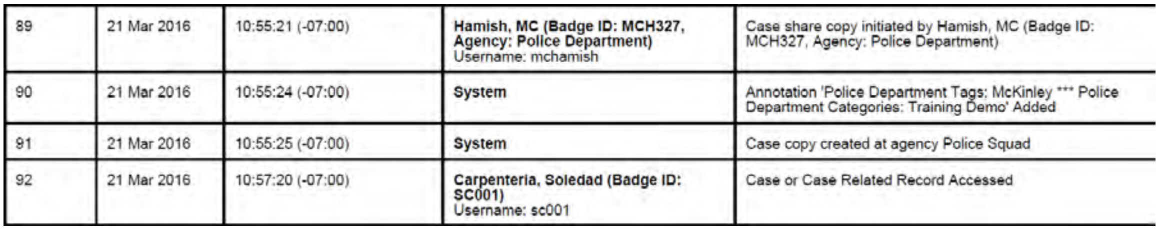
In general, a case shared by a partner agency includes the metadata that the partner agency applied. For some metadata, Evidence.com takes special actions.

- **Case ID** — The ID assigned by the partner agency.
- **Description** — The description assigned by the partner agency.
- **Categories** — None. Evidence.com does not apply a retention category to the case. Evidence.com adds a note to the case to record any retention categories that the partner agency applied to the original case. Because retention policies vary among agencies, Evidence.com does not attempt to determine which of your agency's retention categories should be applied to a case received from a partner agency.
- **Tags** — The tags applied by the partner agency, with the partner agency name appended. For example, if the partner agency applied the tag "McKinley", the copy of the case that you receive includes the tag "McKinley (*partner agency name*)". The tags are also added as notes to the case, to ensure that there is a record of the tags that were received. You can delete the tags that were copied from the partner agency.
- **Notes** — The notes created by the partner agency, with the partner agency name added. Evidence.com adds notes to record the tags and categories that the partner agency had applied to the original case.

Audit Logs

If the partner agency does not include audit logs in the shared case, the case audit log in your agency includes only the entries for actions taken in your agency.

If the partner agency includes audit logs in the shared case, the case audit log in your agency includes all audit log entries from the partner agency in addition to the entries for actions taken in your agency.



89	21 Mar 2016	10:55:21 (-07:00)	**Hamish, MC (Badge ID: MCH327, Agency: Police Department)** Username: mchamish	Case share copy initiated by Hamish, MC (Badge ID: MCH327, Agency: Police Department)
90	21 Mar 2016	10:55:24 (-07:00)	**System**	Annotation 'Police Department Tags: McKinley *** Police Department Categories: Training Demo' Added
91	21 Mar 2016	10:55:25 (-07:00)	**System**	Case copy created at agency Police Squad
92	21 Mar 2016	10:57:20 (-07:00)	**Carpenteria, Soledad (Badge ID: SC001)** Username: sc001	Case or Case Related Record Accessed

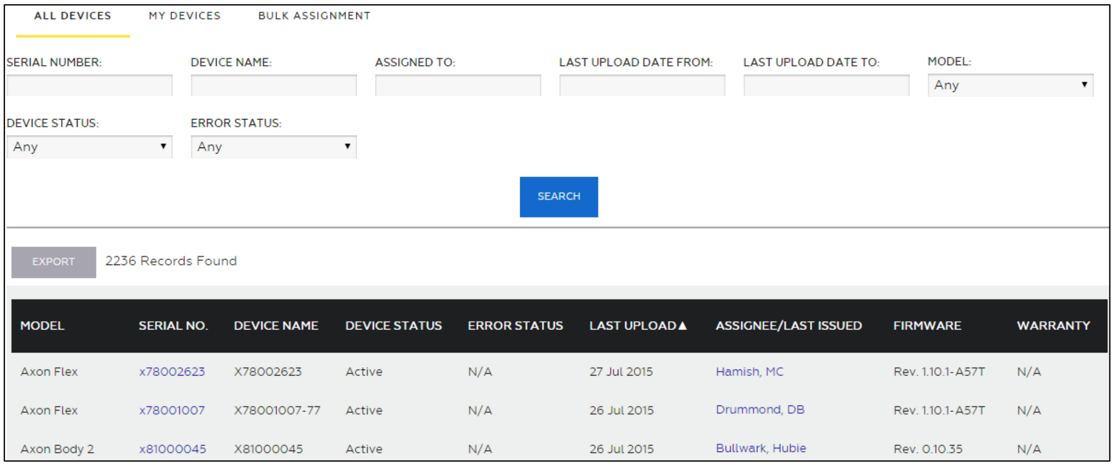
Device Management

Administrators and users who are allowed the Device Administration permission can manage TASER devices by using the Devices menu options.

Device Search — All Devices and My Devices

Evidence.com provides device search features to help you find the devices that you need. In the Devices area, you can use either of the two device-search pages:

- **All Devices**—Finds all devices.
- **My Cases**—Finds devices that are assigned to you. The Assigned To filter is automatically set to your name.



SERIAL NUMBER:

DEVICE NAME:

ASSIGNED TO:

LAST UPLOAD DATE FROM:

LAST UPLOAD DATE TO:

MODEL: Any

DEVICE STATUS: Any

ERROR STATUS: Any

2236 Records Found

MODEL	SERIAL NO.	DEVICE NAME	DEVICE STATUS	ERROR STATUS	LAST UPLOAD ▲	ASSIGNEE/LAST ISSUED	FIRMWARE	WARRANTY
Axon Flex	x78002623	X78002623	Active	N/A	27 Jul 2015	Hamish, MC	Rev. 1.10.1-A57T	N/A
Axon Flex	x78001007	X78001007-77	Active	N/A	26 Jul 2015	Drummond, DB	Rev. 1.10.1-A57T	N/A
Axon Body 2	x81000045	X81000045	Active	N/A	26 Jul 2015	Bullwark, Hubie	Rev. 0.10.35	N/A

1. On the menu bar, click **Devices**.

   The All Devices page lists all devices, sorted by the Last Upload date.

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

Task	Steps
View a device	Click the serial number of the device.
Find devices that are assigned to you	Click **My Devices**.
Find devices assigned to another person.	1. In the **Assigned To** box, enter the name of person whose devices you want to see. 2. Click **Search**.
Find unassigned devices.	1. In the **Assigned To** box, enter “Unassigned” as the name of the person whose devices you want to see. 2. Click **Search**.
Change search results	1. Update the device search filters. For more information, see Device Search Filters. 2. Click **Search**.
Sort search results	Click the column heading for **Serial No**, **Device Name**, **Device Status**, **Error Status**, **Last Upload**, **Firmware**, or **Warranty**. To reverse the sort order, click the heading again.

For information about the actions you can take from search results, see Working with Case Search Results.

Device Search Filters

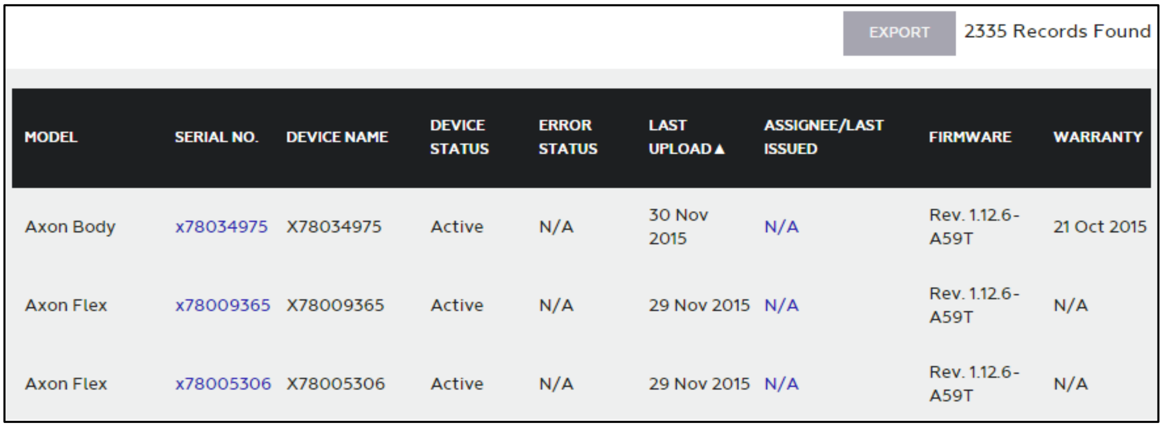
Case search filters help you limit search results to the cases that you want to see. Evidence.com includes in search results only the cases that match *all* the search filters that you set.

- **Serial Number** — Limits search results to devices whose TASER-assigned serial number includes the characters you enter in this box. This filter supports partial matches. For example, if you entered `x7801`, the search results would include the devices with the serial numbers x78017802 and x78017049
- **Device Name** — Limits search results to devices whose name includes the characters you enter in the Device Name box. By default, device names are the same as the device serial number; however, agencies can assign custom device names. This filter supports partial matches.
- **Assigned To** — Limits the search to devices that were most recently assigned to the user you specify.

  To search for unassigned devices, specify "Unassigned" in the Assigned To filter.
- **Last Upload Date From** — Limits the search results to devices that have uploaded to Evidence.com *after* the date specified by this filter.
- **Last Upload Date To** — Limits the search results to devices that have uploaded to Evidence.com *before* the date specified by this filter.
- **Model** — Limits the search results to devices of the type that you specify.
- **Device Status** — Limits the search results to devices whose overall status is the same as the status you specify.
- **Error Status** — Limits the search results to devices whose error status is the same as the status you specify.

Working with Device Search Results

On device search pages — All Devices and My Devices — you can take the actions described in this section.



2335 Records Found

MODEL	SERIAL NO.	DEVICE NAME	DEVICE STATUS	ERROR STATUS	LAST UPLOAD ▲	ASSIGNEE/LAST ISSUED	FIRMWARE	WARRANTY
Axon Body	x78034975	X78034975	Active	N/A	30 Nov 2015	N/A	Rev. 1.12.6-A59T	21 Oct 2015
Axon Flex	x78009365	X78009365	Active	N/A	29 Nov 2015	N/A	Rev. 1.12.6-A59T	N/A
Axon Flex	x78005306	X78005306	Active	N/A	29 Nov 2015	N/A	Rev. 1.12.6-A59T	N/A

View Device Profile

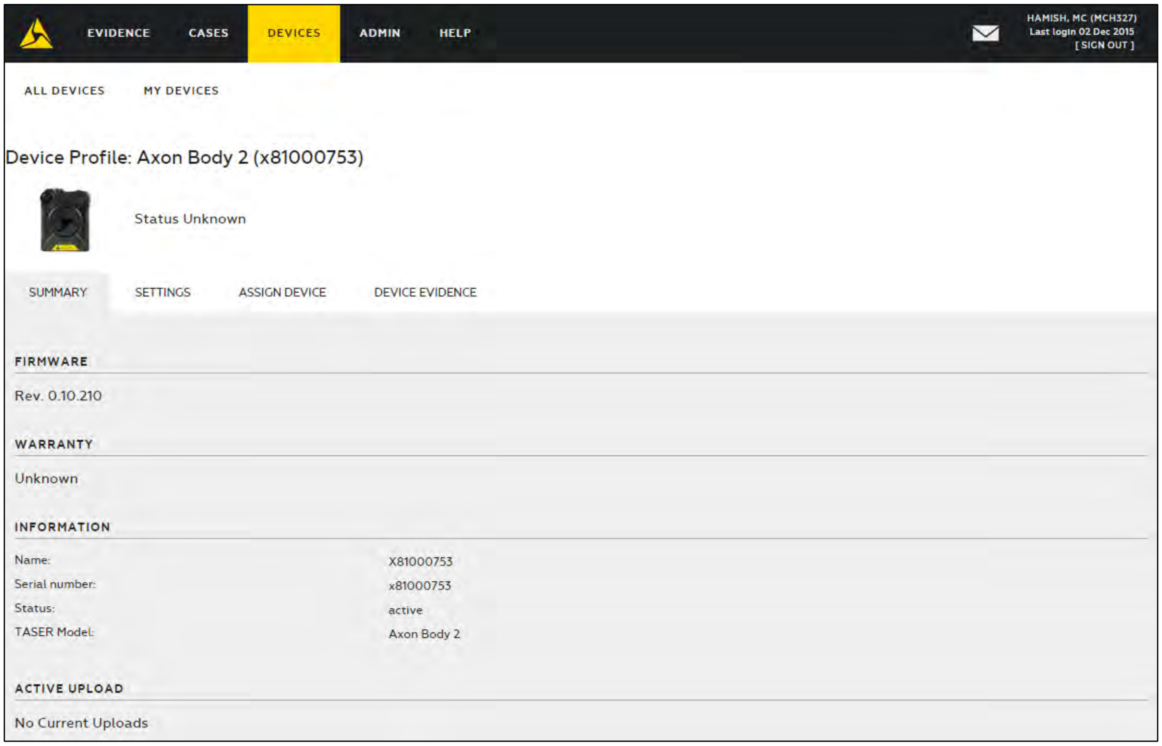
1. Search for the device you want to view.
2. In the search results, click the serial number of the device.

   The Device Profile page opens.

   By default, the Summary tab is selected. This tab shows essential information about the device, such as the firmware version and warranty information. If the device is currently uploading videos to Evidence.com, video upload progress appears under Active Upload.

   For TASER CEWs, an Event Info tab is included on the Device Profile page. This tab displays the firing log information of the device.

For information about the actions you can take from the Device Profile page, see Working with a Device.



Device Profile: Axon Body 2 (x81000753)

Status Unknown

FIRMWARE

Rev. 0.10.210

WARRANTY

Unknown

INFORMATION

Name:	X81000753
Serial number:	x81000753
Status:	active
TASER Model:	Axon Body 2

ACTIVE UPLOAD

No Current Uploads

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/Last Issued**, 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, Microsoft Excel, text, or CSV format.

If the search results contain more than 500 devices, Evidence.com exports the search results in 500-device segments and asks you to confirm the download of the next segment.

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

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

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

   The device search results download in the format that you specified.

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

4. If you want to export device search results for additional devices, click **OK** each time the dialog box appears.

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

Working with a Device

This section describes the actions available on the Device Profile page.

Edit Device Settings

For most device types, you can change the device name.

For Axon Flex, you can specify the device orientation.

For Axon Body 2, you can configure the speaker volume, whether the camera vibrates, and whether the camera is in stealth mode.

1. On the Device Profile page, click the **Settings** tab.

2. Edit the settings as needed.

3. Click **Save Settings**.

Assign a Device

For most device types, you can use the Device Profile page to assign the device to a user

1. On the Device Profile page, click the **Assign Device** tab.
2. In the **Assign Device To** box, start typing the name of the user who you want to assign the device to, wait for Evidence.com to show the matching users, and then click the user you want. You can also type the user badge ID.
3. Click **Assign Device**.

   Evidence.com assigns the device to the user you selected.

View Evidence Created by a Device

Any evidence recorded on the device that has been uploaded to Evidence.com appears on the Device Evidence tab.

1. On the Device Profile page, click the **Device Evidence** tab.

   Evidence.com shows a list of all evidence uploaded from the device.

2. Use the evidence list as needed. The following table provides concise steps for the tasks you can perform from the evidence list.

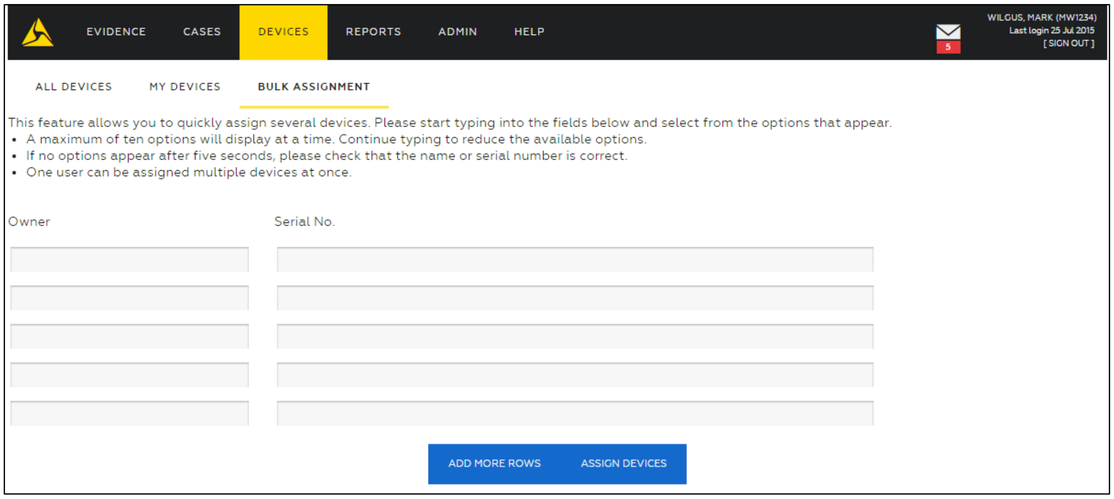
Task	Steps
Add evidence ID	When evidence does not have an ID assigned, “Add” appears in the ID column. If you want to add an ID to evidence: 1. In the ID column, click **Add**. A dialog box appears. 2. In the **Enter ID** box, enter the ID that you want to assign to the evidence, and then click **Save**.
View evidence	In the **Title** column, click the title of the evidence. The View Evidence page displays information about the evidence. For more information about actions available from the View Evidence page, see Working with Any Evidence.
View evidence owner	In the **Owner** column, click the name of the evidence owner. The User Summary page displays information about the user.
View evidence audit trail	In the **Actions** column, click ≣. For more information, see View Evidence Audit Trail.
Download evidence file	In the **Actions** column, click ⬇. For more information, see Download Evidence File.
Flag or un-flag evidence	In the **Actions** column, click ⚑. For more information, see Flag or Un-Flag Evidence.

Bulk Assign Devices

Using the Bulk Assignment feature, you can assign devices to many users at once.

1. On the menu bar, click **Devices** and then click **Bulk Assignment**.

   The Device Bulk Assignment page appears.



This feature allows you to quickly assign several devices. Please start typing into the fields below and select from the options that appear.

- 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.
- One user can be assigned multiple devices at once.

2. In the first box 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.

3. In the first box 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.

4. For each additional device that you need to assign, repeat the previous two steps. If you need more rows, click **Add More Rows**.

5. When you are done specifying users and the devices to assign to them, click **Assign Devices**.

   A notification message box appears.

6. Click **OK**.

   Evidence.com assigns the devices to the users that you specified.

7. If you want to verify that the devices are correctly assigned, use the All Devices page to search for each device by serial number and then view the Assignee name in the search results.

Axon Device Manager for Axon Body 2 Cameras

The Axon Device Manager app for Android simplifies and accelerates device assignment of Axon Body 2 cameras. Axon Device Manager runs on Android devices that are equipped with an NFC antenna. With the app running, the armorer taps the back of the Android device to an Axon Body 2 camera and receives 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 camera.

To install Axon Device Manager on an Android device, go to the Google Play store (https://play.google.com/store) and search for Axon Device Manager.

Reporting

Evidence.com allows administrators and those with the reporting permission to generate reports showing Evidence.com utilization. These options can help your agency turn that data into valuable answers to ensure your Evidence.com account is providing you with the flexibility and utility your agency deserves.

Evidence.com reports are spreadsheets that can be opened by many spreadsheet applications. Reports include all relevant metadata for the items included in the report. Using the Microsoft Excel pivot table function, you can group evidence by any of the fields, such as owner or badge ID, to get a better understanding of individual officer usage or certain category retentions over a given period. For more information, see Example Data Aggregation Using Microsoft Excel Pivot Tables.

The reports available are the following:

- **Evidence Created** — Lists all evidence on your agency's account in order of when the data was created. It also lists all associated metadata attached to those pieces of evidence.
- **Evidence Deleted** — Lists all evidence deleted and associated metadata on your agency's account in order of when the data was deleted. This report provides better monitoring of automated deletions and help ensure a proper retention policy is in place.
- **Category Summary** — Lists the current count of total files and file size in megabytes (MB) for each category as well as the percent of files assigned to that category.
- **Uncategorized Evidence** — Lists users with uncategorized evidence assigned to them. A second tab on the export lists every piece of uncategorized evidence and includes the owner information, evidence title, date recorded, and link to the evidence.

- **User Summary** — Lists total files and file size in MB, broken out by owner of the evidence. The counts are further broken out by evidence type, active, and deleted evidence.

- **Axon Video Summary** — Lists usage metrics on Axon videos uploaded to your agency. The first tab is a summary of Number of videos, hours, and MB uploaded. The second tab breaks out the uploads by the specified grouping: Day, Month, or Year.

- **Sharing Audit Report** — Lists all user actions related to sharing evidence and cases. Included in the report are details such as the following examples:

  - 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

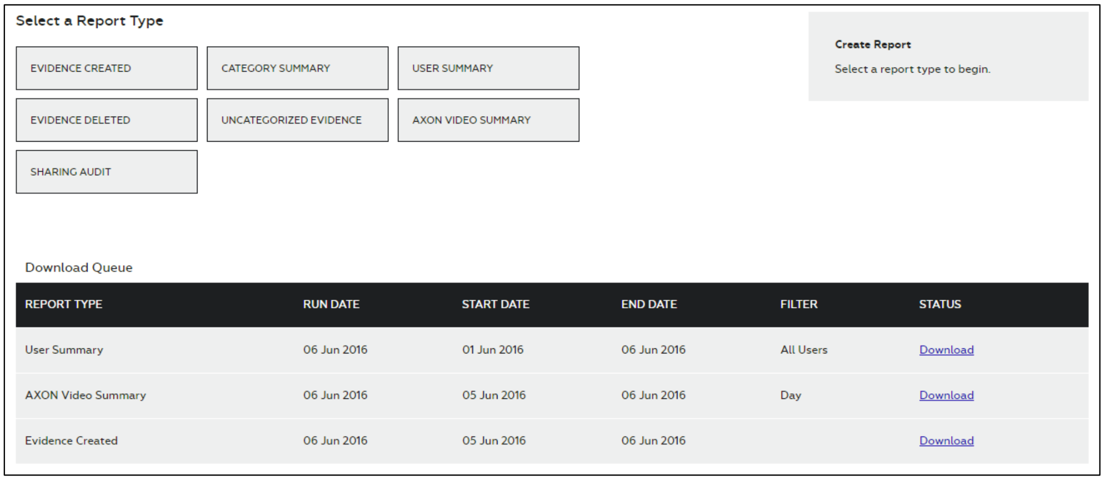
Run a Report

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.



Select a Report Type

Create Report

Select a report type to begin.

Download Queue

REPORT TYPE	RUN DATE	START DATE	END DATE	FILTER	STATUS
User Summary	06 Jun 2016	01 Jun 2016	06 Jun 2016	All Users	Download
AXON Video Summary	06 Jun 2016	05 Jun 2016	06 Jun 2016	Day	Download
Evidence Created	06 Jun 2016	05 Jun 2016	06 Jun 2016		Download

2. Under **Select a Report Type**, click the report that you want to run.

   Depending on the report type, additional report options appear.

3. If the Select A Summary Type report options appears, do one of the following:

   - If you want a User Summary report for all users, click **All Users**.
   - If you want a User Summary report for one user only, click **Single User** and then in the **Reassign To** box, start typing the name of the user, wait for Evidence.com to show the matching users, and then click the user you want.

4. If the Select a Date Range report options appear and you want to change the date range, do one of the following:

   - If you want to use a standard date range, click the link for the date range you want.
   - If you want to set a custom date range, in the From and To boxes, type the dates or click the calendar icon and choose the dates.

5. If the Filter report options appear, click the grouping option that you want.

6. Under Create Report, verify that the report configuration is what you want. If not, modify the report options.

7. Click **Run Report**.

   Under Download Queue, the report is listed, as either Running, Failed, or Download.

   When the report is ready, Evidence.com sends you a notification email that includes a download link.

8. If the report status is Download, click **Download**.

Downloading Reports

You can download reports either by visiting the Reports page or by the download link in a notification email.

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.

Help Section

All Evidence.com users can access the Help section to view the help text, release notes, and user guides; to download Evidence Sync and Axon Capture; or to contact TASER with questions or comments.

Help Center

The Help Center page provides basic information about the various features of Evidence.com and of Evidence Sync.

1. On the menu bar, click **Help** and then click **Help Center**.
2. Click the tab for the product that you want help with — Evidence.com or Evidence Sync.

   Headings for the available help topics appear below the tab.
3. To open a help topic, click the topic title.

Release Notes and User Guides

The Notes and Guides page displays links to the Evidence.com release notes and user guides.

The Release Notes section lists the release notes for each previous version of Evidence.com, in reverse chronological order.

The User Guides sections displays links to the most recent version of the available guides.

Release notes and user guides are in PDF format.

1. On the menu bar, click **Help** and then click **Release Notes / User Guides**.

   The Release Notes and User Guides sections list links to the various documents.
2. To access a document, click a link.

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

Download and Install Evidence Sync

You can download the current version of the Evidence Sync application from the Downloads page. Using Evidence Sync for Windows, you can manage and upload data from your TASER X2, TASER X3, TASER X26, TASER X26P, TASER CAM, TASER CAM HD, Axon Flex, Axon Body, and Axon Body 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 (C:\Program Files\TASER International).
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.

Contact Us

The Contact Us page displays TASER contact information. If you or your agency's Evidence.com users have any questions or queries regarding TASER products and services, you can contact TASER 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 TASER can provide you an accurate and precise response.
5. Click **Submit**.
6. On the notification message box, click **OK**.

Appendix A: Roles and Permissions

The following topics provide a reference for the Roles and Permissions feature. For more information about this feature, see Roles and Permissions.

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.

Permissions Supported by Evidence.com	Supported by Agency Types	Unlocked By	Description
Login Access			
Evidence.com	PRO and LITE	—	Allows a user to log in to their agency's Evidence.com agency.
Evidence Sync	PRO and LITE	—	Allows a user to log in to Evidence Sync in Online mode.
Axon Capture	PRO and LITE	—	Allows a user to log in to the Axon Capture mobile application.
User Account			
Edit Account Information	PRO and LITE	User Administration	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 & Compose User Messages	PRO and LITE	User Search	Allows a user to read and send messages to other users.
Download Sync Software	PRO and LITE	—	Allows a user to download Sync software from their Evidence.com agency.
Create/Edit Group	PRO and LITE	User Search	Allows a user to create a group, and edit its monitors and members.
Group Audit Trail PDF	PRO and LITE	—	Allows a user to view an audit trail of the activities related to a group.
Admin Access			
Configure Agency Security Settings	PRO and LITE	—	Allows a user to edit the agency's IP Restrictions, authentication method, password configurations, and partner agencies.

Permissions Supported by Evidence.com	**Supported by Agency Types**	**Unlocked By**	**Description**
Edit Agency Settings	PRO and LITE	—	Allows a user to configure agency wide settings including Categories and Retention, Video and Camera Settings, Roles and Permissions, and Password Configuration requirements.
Edit Device Offline & Microphone Settings	PRO and LITE	—	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.
Device Administration	PRO and LITE	Device Search	Allows a user to reassign all agency devices, change their settings, and upload any CEW logs.
User Administration	PRO and LITE	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).
Category Administration	PRO and LITE	—	Allows a user to add a Category to the agency's list or edit an existing Category
Generate Reports	PRO Only	Evidence View: Any Evidence	Allows a user to generate reports.
Search Access			
User Search	PRO and LITE	—	Allows a user to see what users are in the agency. If disabled the user are unable to see any evidence or devices assigned to others, assign devices or evidence to others, share evidence or cases, or send messages to others.
Partner Contact Search	PRO Only	—	Allows a user to view members of partner agencies that have been added to your agency's contact list Unlocks: Share Externally to Authenticated Users, Share With Partner Agencies
Evidence Search	PRO and LITE	User Search	Allows a user to search for all of the Evidence in the agency. Note: the user can only access the Evidence specified under the Evidence Management permissions.
Device Search	PRO and LITE	User Search	Allows a user to search for all of the Devices in the agency.
Case Search	PRO Only	Evidence Search	Allows a user to search for all of the Cases in an agency. Note: Their ability to access a Case is determined by the Case Management Permissions.

Permissions Supported by Evidence.com	**Supported by Agency Types**	**Unlocked By**	**Description**
Evidence Creation			
Upload External Files	PRO and LITE	—	Allows a user to upload files through Evidence Sync, Axon Capture, and the Import Evidence feature. This does not affect the ability to upload through an ETM or Evidence.com Dock.
Configure Automatic Upload through Evidence Sync	PRO and LITE	Upload External Files	Allows a user to configure Automatic Upload through Evidence Sync.
Evidence Management			
View	PRO and LITE	—	Allows a user to access evidence. Does not include weapon firing logs.
View CEW Firing Logs	PRO and LITE	—	Allows a user to view weapon firing logs.
Edit	PRO and LITE	Evidence View	Allows a user to change the Title, ID, Flag, Assignment, Category, Tags and Location.
Add/Remove Pending Review Category	PRO and LITE	Evidence Edit	Allows a user to add or remove the Pending Review Category from a piece of Evidence.
Redact	PRO Only	Evidence Edit	Allows a user to create redactions of video evidence files. This does not alter the original video in any way.
Reassign	PRO and LITE	Evidence View	Allows a user to change the owner of an evidence file.
Delete Evidence & Edit Date Recorded	PRO and LITE	Evidence View	Allows a user to manually initiate the deletion of Evidence before its Category determined date.
Download	PRO and LITE	Evidence View	Allows a user to download Evidence.
Share	PRO Only	View Evidence (User Search should also be allowed)	Allows a user to allow other users to have access to Evidence.
Share Externally to Authenticated Users	PRO Only	Partner Contact Search, Evidence 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 logs. If they do not have an Evidence.com account, they can create a free guest account on my.evidence.com.

Permissions Supported by Evidence.com	Supported by Agency Types	Unlocked By	Description
Share External Download Links	PRO Only	Evidence Share	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 logs.
Post Notes	PRO and LITE	Evidence View	Allows a user to write messages associated with Evidence.
Audit Trail PDF	PRO and LITE	Evidence View	Allows a user to view and download the record of who has Viewed or Edited Evidence.
Restricted Category Access	PRO Only	Evidence View	Allows a user to access Evidence that has been categorized as Restricted Access.
Case Management			
View	PRO Only	—	Allows a user to access a Case
Edit	PRO Only	Case View	Allows a user to Edit Case ID, Description, Categories, Tags, and Folder Structure.
Reassign	PRO Only	Case Edit (User Search should also be allowed)	Allows a user to change the Owner of a piece of a Case.
Share	PRO Only	Case View (User Search should also be allowed)	Allows a user to add members to a Case, giving them access to the associated Evidence.
Share with Partner Agencies	PRO Only	Partner Contact Search, Case Share, Evidence View: Any Evidence, Evidence Download, Evidence Share, 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 logs.
Share External Download Links	PRO Only	Case Share, Evidence View: Any Evidence, Evidence Download, Evidence Share, Evidence 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 log 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 logs.
Audit Trail PDF	PRO Only	Case View	Allows a user to view and download the record of who has Viewed or Edited a Case.

Permissions Supported by Evidence.com	**Supported by Agency Types**	**Unlocked By**	**Description**
View & Add Case Notes	PRO Only	Case View	Allows a user to write messages associated with a Case.
Create Case	PRO Only	Case View	Allows a user to create a Case.
Restricted Category Access	PRO Only	Case View	Allows a user to access Cases that have been categorized as Restricted Access.
Shared Case			
View	PRO Only	—	Allows users to access a Case that has been Shared with them.
Edit	PRO Only	Shared Case View	Allows users to Edit Case ID, Description, Categories, Tags, and Folder Structure of a Case that has been shared with them.
Reassign	PRO Only	Shared Case View (User Search should also be allowed)	Allows a user to reassign a Case that has been Shared with them.
Share	PRO Only	Shared Case View (User Search should also be allowed)	Allows users to add members to a Case that has been shared with them, giving access to the associated Evidence.
View & Add Case Notes	PRO Only	Shared Case View	Allows users to write messages associated with a Case that has been Shared with them.
Audit Trail PDF	PRO Only	Shared Case View	Allows users to view and download the record of who has Viewed or Edited a Case that has been shared with them.
Email Notification Preferences			
Account Lockout Notification	PRO and LITE	User Administration (User Search should also be allowed)	Determines whether or not a user receives Account Lockout Notifications when any user in the agency is locked out.
Upcoming Evidence Deletion Notification	PRO and LITE	User Administration (User Search should also be allowed)	Determines whether or not a user receives weekly notifications of any upcoming evidence deletions in the agency.
Evidence Timestamp Notification	PRO and LITE	User Administration	Determines whether or not a user receives weekly notifications of evidence whose timestamp indicates it is older than 14 days.

PRO Agency Pre-Configured Roles and Default Permissions

The following table provides the default permissions for the preconfigured roles of an Evidence.com PRO account.

Permissions in Evidence.com PRO Agencies	Admin	User	Investigator	Armorer	Assignee Only
Login Access					
Evidence.com	Allowed	Allowed	Allowed	Allowed	Prohibited
Evidence Sync	Allowed	Allowed	Allowed	Allowed	Prohibited
Axon Capture	Allowed	Allowed	Allowed	Allowed	Prohibited
User Account					
Edit Account Information	Allowed	Allowed	Allowed	Allowed	Prohibited
View & Compose User Messages	Allowed	Prohibited	Allowed	Allowed	Prohibited
Download Sync Software	Allowed	Allowed	Allowed	Allowed	Prohibited
Create/Edit Group	Allowed	Prohibited	Prohibited	Prohibited	Prohibited
Group Audit Trail PDF	Allowed	Prohibited	Prohibited	Prohibited	Prohibited
Admin Access					
Configure Agency Security Settings	Allowed	Prohibited	Prohibited	Prohibited	Prohibited
Edit Agency Settings	Allowed	Prohibited	Prohibited	Prohibited	Prohibited
Edit Device Offline & Microphone Settings	Allowed	Prohibited	Prohibited	Prohibited	Prohibited
Device Administration	Allowed	Prohibited	Prohibited	Allowed	Prohibited
User Administration	Allowed	Prohibited	Allowed	Prohibited	Prohibited
Category Administration	Allowed	Prohibited	Prohibited	Prohibited	Prohibited
Generate Reports	Allowed	Prohibited	Prohibited	Prohibited	Prohibited
Search Access					
User Search	Allowed	Allowed	Allowed	Allowed	Prohibited
Partner Contact Search	Allowed	Prohibited	Prohibited	Prohibited	Prohibited
Evidence Search	Allowed	Allowed	Allowed	Allowed	Prohibited
Device Search	Allowed	Allowed	Allowed	Allowed	Prohibited
Case Search	Allowed	Allowed	Allowed	Allowed	Prohibited
Evidence Creation					
Upload External Files	Allowed	Allowed	Allowed	Allowed	Prohibited
Configure Automatic Upload through Evidence Sync	Allowed	Prohibited	Prohibited	Prohibited	Prohibited
Evidence Management					
View	Any Evidence	Only Their Own	Only Their Own	Only Their Own	Prohibited

Permissions in Evidence.com PRO Agencies	**Admin**	**User**	**Investigator**	**Armorer**	**Assignee Only**
View CEW Firing Logs	Any Evidence	Only Their Own	Only Their Own	Only Their Own	Prohibited
Edit	Any Evidence	Only Their Own	Only Their Own	Only Their Own	Prohibited
Add/Remove Pending Review Category	Any Evidence	Prohibited	Prohibited	Prohibited	Prohibited
Redact	Any Evidence	Only Their Own	Only Their Own	Only Their Own	Prohibited
Reassign	Any Evidence	Only Their Own	Only Their Own	Only Their Own	Prohibited
Delete Evidence & Edit Date Recorded	Any Evidence	Prohibited	Prohibited	Prohibited	Prohibited
Download	Any Evidence	Only Their Own	Only Their Own	Only Their Own	Prohibited
Share	Any Evidence	Only Their Own	Only Their Own	Only Their Own	Prohibited
Share Externally to Authenticated Users	Allowed	Prohibited	Prohibited	Prohibited	Prohibited
Share External Download Links	Allowed	Prohibited	Prohibited	Prohibited	Prohibited
Post Notes	Any Evidence	Only Their Own	Only Their Own	Only Their Own	Prohibited
Audit Trail PDF	Any Evidence	Only Their Own	Only Their Own	Only Their Own	Prohibited
Restricted Category Access	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited
Case Management					
View	Any Cases	Only Their Own	Any Cases	Only Their Own	Prohibited
Edit	Any Cases	Only Their Own	Any Cases	Only Their Own	Prohibited
Reassign	Any Cases	Only Their Own	Any Cases	Only Their Own	Prohibited
Share	Any Cases	Only Their Own	Any Cases	Only Their Own	Prohibited
Share with Partner Agencies	Allowed	Prohibited	Prohibited	Prohibited	Prohibited
Share External Download Links	Allowed	Prohibited	Prohibited	Prohibited	Prohibited
Audit Trail PDF	Any Cases	Only Their Own	Any Cases	Only Their Own	Prohibited
View & Add Case Notes	Any Cases	Only Their Own	Any Cases	Only Their Own	Prohibited
Create Case	Allowed	Prohibited	Allowed	Allowed	Prohibited
Restricted Category Access	Prohibited	Prohibited	Prohibited	Prohibited	Prohibited

Permissions in Evidence.com PRO Agencies	Admin	User	Investigator	Armorer	Assignee Only
Shared Case					
View	Allowed	Allowed	Allowed	Allowed	Prohibited
Edit	Allowed	Allowed	Allowed	Allowed	Prohibited
Reassign	Allowed	Allowed	Allowed	Allowed	Prohibited
Share	Allowed	Allowed	Allowed	Allowed	Prohibited
View & Add Case Notes	Allowed	Allowed	Allowed	Allowed	Prohibited
Audit Trail PDF	Allowed	Allowed	Allowed	Allowed	Prohibited
Email Notification Preferences					
Account Lockout Notification	Allowed	Prohibited	Prohibited	Prohibited	Prohibited
Upcoming Evidence Deletion Notification	Allowed	Prohibited	Prohibited	Prohibited	Prohibited
Evidence Timestamp Notification	Allowed	Prohibited	Prohibited	Prohibited	Prohibited

LITE Agency Pre-Configured Roles and Default Permissions

The following table provides the default permissions for the preconfigured roles of an Evidence.com LITE account. Permissions for features that are not supported in Evidence.com LITE agencies are marked with N/A.

Permissions in Evidence.com LITE Agencies	Lite Admin	Lite User	Lite Armorer	Assignee Only
Login Access				
Evidence.com	Allowed	Allowed	Allowed	Prohibited
Evidence Sync	Allowed	Allowed	Allowed	Prohibited
Axon Capture	Allowed	Allowed	Allowed	Prohibited
User Account				
Edit Account Information	Allowed	Allowed	Allowed	Prohibited
View & Compose User Messages	Allowed	Allowed	Allowed	Prohibited
Download Sync Software	Allowed	Allowed	Allowed	Prohibited
Create/Edit Group	Prohibited	Prohibited	Prohibited	Prohibited
Group Audit Trail PDF	Prohibited	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
Device Administration	Allowed	Prohibited	Allowed	Prohibited

Permissions in Evidence.com LITE Agencies	**Lite Admin**	**Lite User**	**Lite Armorer**	**Assignee Only**
User Administration	Allowed	Prohibited	Prohibited	Prohibited
Category Administration	Allowed	Prohibited	Prohibited	Prohibited
Generate Reports	N/A	N/A	N/A	N/A
Search Access				
User Search	Allowed	Allowed	Allowed	Prohibited
Partner Contact Search	Prohibited	Prohibited	Prohibited	Prohibited
Evidence Search	Allowed	Prohibited	Prohibited	Prohibited
Device Search	Allowed	Prohibited	Allowed	Prohibited
Case Search	N/A	N/A	N/A	N/A
Evidence Creation				
Upload External Files	Allowed	Allowed	Allowed	Prohibited
Configure Automatic Upload through Evidence Sync	Allowed	Prohibited	Prohibited	Prohibited
Evidence Management				
View	Any Evidence	Only Their Own	Only Their Own	Prohibited
View CEW Firing Logs	Any Evidence	Only Their Own	Only Their Own	Prohibited
Edit	Any Evidence	Only Their Own	Only Their Own	Prohibited
Add/Remove Pending Review Category	Any Evidence	Prohibited	Prohibited	Prohibited
Redact	N/A	N/A	N/A	N/A
Reassign	Any Evidence	Prohibited	Prohibited	Prohibited
Delete Evidence & Edit Date Recorded	Any Evidence	Prohibited	Prohibited	Prohibited
Download	Any Evidence	Only Their Own	Only Their Own	Prohibited
Share	N/A	N/A	N/A	N/A
Share Externally to Authenticated Users	N/A	N/A	N/A	N/A
Share External Download Links	N/A	N/A	N/A	N/A
Post Notes	Any Evidence	Only Their Own	Only Their Own	Prohibited
Audit Trail PDF	Any Evidence	Only Their Own	Only Their Own	Prohibited
Restricted Category Access	N/A	N/A	N/A	N/A
Case Management				
View	N/A	N/A	N/A	N/A
Edit	N/A	N/A	N/A	N/A

Permissions in Evidence.com LITE Agencies	**Lite Admin**	**Lite User**	**Lite Armorer**	**Assignee Only**
Reassign	N/A	N/A	N/A	N/A
Share	N/A	N/A	N/A	N/A
Share with Partner Agencies	N/A	N/A	N/A	N/A
Share External Download Links	N/A	N/A	N/A	N/A
Audit Trail PDF	N/A	N/A	N/A	N/A
View & Add Case Notes	N/A	N/A	N/A	N/A
Create Case	N/A	N/A	N/A	N/A
Restricted Category Access	N/A	N/A	N/A	N/A
Shared Case				
View	N/A	N/A	N/A	N/A
Edit	N/A	N/A	N/A	N/A
Reassign	N/A	N/A	N/A	N/A
Share	N/A	N/A	N/A	N/A
View & Add Case Notes	N/A	N/A	N/A	N/A
Audit Trail PDF	N/A	N/A	N/A	N/A
Email Notification Preferences				
Account Lockout Notification	Allowed	Prohibited	Prohibited	Prohibited
Upcoming Evidence Deletion Notification	Allowed	Prohibited	Prohibited	Prohibited
Evidence Timestamp Notification	Allowed	Prohibited	Prohibited	Prohibited

Appendix B: Traditional Media Player

Beginning with release 1.27, a new media player is the default player; however, users who want to use the traditional Evidence.com media player and redaction tools can switch to the traditional player and tools as needed.

For information about using the new media player, see Playing Video and Audio Evidence.

Working with Video and Audio Evidence

This section describes the actions available on the View Evidence page for video and audio files when you use the traditional media player.

Actions available for all files types are described in Working with Any Evidence.

Play, Pause, Rewind, and Fast Forward

On the View Evidence page, the video and audio player each provide the following basic functions:

- Play — Click anywhere on the player or, below the player, click ▶ (play).
- Pause — Click anywhere on the player or, below the player, click ❚❚ (pause).
- Rewind — Below the player, click «. Each click rewinds the file approximately 4% of its overall length.
- Fast Forward — Below the player, click ». Each click fast forwards the video approximately 4% of its total length.

Show and Hide Clock

In addition to the clock shown below the video image, you can show or hide the clock in the video image itself.

To show or hide the clock, on the toolbar, click 🕒.

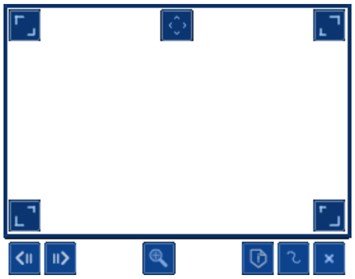
Magnify Zone

You can use the zone magnification tool to zoom in on a portion of a video frame. You have the option of converting a magnified zone into a marker.

1. Play the video to about the frame that you want to magnify and then click ❚❚ (pause). You can pick the exact first frame more easily later.

2. From the tool bar, click 🔍 (magnify zone).

   The zone magnification tool appears over the player.



3. Use the zone magnification tool as needed to view details in the video.

   - To move the tool, at the top center of the tool, click and hold ⛶ and then drag the tool to where you need.
   - To resize the tool, click and hold one of the corners (⌟, ⌞, ⌜ or ⌝) and then drag the corner until the tool is the size and shape that you need.
   - To skip backwards or forwards one second, click <II or II>.
   - To expand what is inside the rectangle of the tool, at the bottom of the tool, click 🔍.
   - To return to full frame from the expanded tool, at the bottom of the video image, click ✕.
   - To add or remove pixel smoothing, click ∿ or ⎍.

4. If you want to save the magnified area as a marker, click ⛉.

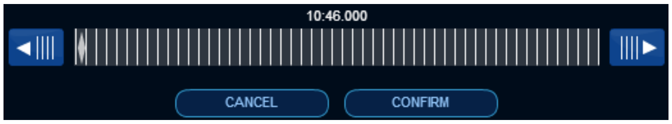
   The Add Marker dialog box appears. For more information, see Add Marker.

View Video Frame by Frame

1. Play the video to about the time that you want to view frame by frame and then click ❙❙ (pause).

2. From the tool bar, click ❙❙❙► (view frame by frame).

   Below the player, the frame-by-frame scrub bar appears. Each segment of the bar represents a video frame.

3. Use the frame-by-frame features as needed:

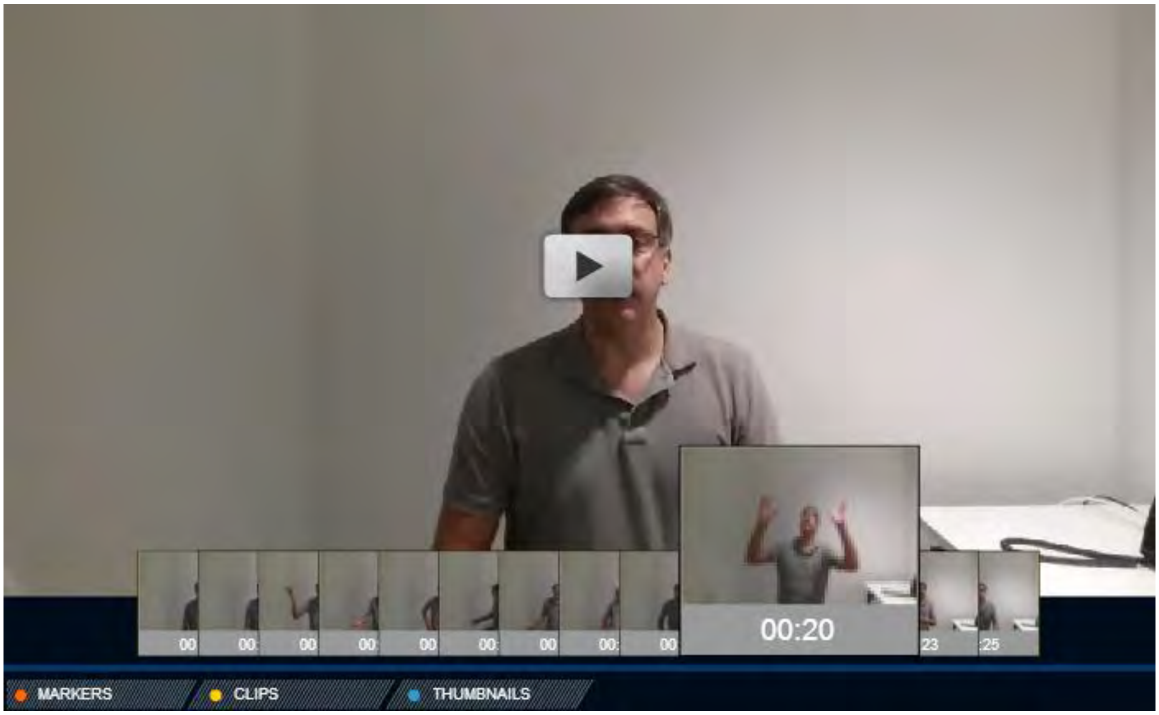
   - To preview frames, hover the mouse pointer over the scrub bar.
   - To go to a frame, click on its segment on the scrub bar.
   - To skip backwards or forwards one second, click ◄❙❙❙ or ❙❙❙► .

4. You can exit frame-by-frame viewing mode in one of two ways:

   - To remain at the last frame you viewed in frame-by-frame mode, click **Continue**.
   - To return to where you were in the video prior to viewing frame by frame, click **Cancel**.

Show and Hide Thumbnails

Thumbnails provide an easy way to preview parts of a video. They appear at the bottom of the video image. You can move the mouse pointer across them to see each thumbnail.



You can also control whether thumbnails appear.

- To hide thumbnails, click ● THUMBNAILS
- To show thumbnails, click ● THUMBNAILS

Rotate the Video

You can rotate the player image 90, 180, or 270 degrees clockwise. This feature is for convenience while viewing a video only. For example, the camera itself may have been on its side or upside down while recording.

The rotation does not affect the original video file and is not saved in any way. The next time you access the video, the video is not rotated.

To rotate the video image 90 degrees clockwise, click ↻.

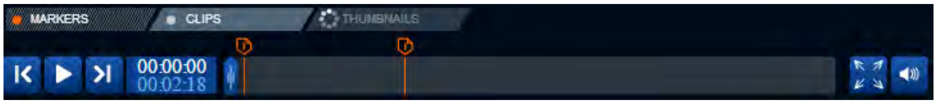
Markers

You can use markers to indicate key moments or highlight important aspects of a video or audio evidence file.

For video markers only, you can download markers as image files. Prior to downloading the marker, you can specify options such as whether the title and description appear on the downloaded image.

Show and Hide Markers

You can control whether the scrub bar, located below the video image, shows red icons for each marker.



- To hide marker icons on the scrub bar, click ● MARKERS
- To show marker icons on the scrub bar, click ● MARKERS

Add Marker

1. On the View Evidence page, below the player, click **Add Marker**.

   The Add Marker dialog box appears over the player.

2. Find the video frame that you want to mark.

   - To move rapidly through the video, on the scrub bar, click and hold ⬆ and then drag it left or right towards the frame that you want to mark.
   - To skip backwards or forwards one second, click <II or II>.

3. In the **Title** box, type the title that you to give the marker.
4. In the **Description** box, type a useful description of what is shown in the marker.
5. Select the marker options that you need.

   - To add fisheye distortion, click 👁.
   - To use pixel smoothing, click ⎍.
   - To make the title, timecode, and description visible in the marker image, click T.

6. Click **Add Marker**.

   The Add Marker dialog box closes.

   The new marker icon appears on the scrub bar at the time where you added the marker.

   Below the player, under Markers, the new marker appears in the list of markers.

Edit Marker

1. On the View Evidence page, below the player and under Markers, find the marker that you want to edit.

2. Click the marker name.

   The player jumps to the marker. In a transparent dialog box over the player, the name and timecode of the marker appear.

3. In the transparent dialog box, click **Edit**.

   The Edit Marker dialog box appears.

4. If you want to change the video frame of the marker, find the video frame that you want to mark.

   - To move rapidly through the video, on the scrub bar, click and hold ▮ and then drag it left or right towards the frame that you want to mark.

   - To skip backwards or forwards one second, click <II or II>.

5. If you want to edit the title, in the **Title** box, type the new title that you to give the marker.

6. If you want to edit the description, in the **Description** box, type a new, useful description of what is shown in the marker.

7. Select the marker options that you need.

   - To add fisheye distortion, click 👁.

   - To use pixel smoothing, click ∼.

   - To make the title, timecode, and description visible in the marker image, click T.

8. Click **Edit Marker**.

   The Add Marker dialog box closes.

The new marker icon appears on the scrub bar at the time where you added the marker.

Below the player, under Markers, the new marker appears in the list of markers.

View Marker

1. On the View Evidence page, below the player and under Markers, find the marker that you want to view.
2. Click the marker name.

   The player jumps to the marker. The name and timecode of the marker appear over the bottom of the video.

Download Marker

You can download a video marker as a PNG file.

1. On the View Evidence page, below the player and under Markers, find the marker that you want to download.
2. To the left of the marker, click ⤓ (download).

   The Download Marker dialog box appears.

3. If you want to modify the title or description or if you want to select marker options, you can do so prior to downloading the marker.

   For more information, see Edit Marker.

4. Click **Download Marker**.
5. Use the dialog box that appears to save the marker to your computer.
6. On the Download Marker dialog box, in the upper-left corner, click ✕ (exit).

Delete Marker

1. On the View Evidence page, below the player and under Markers, find the marker that you want to delete.
2. Click the marker name.

   The player jumps to the marker. In a transparent dialog box over the player, the name and timecode of the marker appear.

3. In the transparent dialog box, click **Delete** and then click **Confirm**.

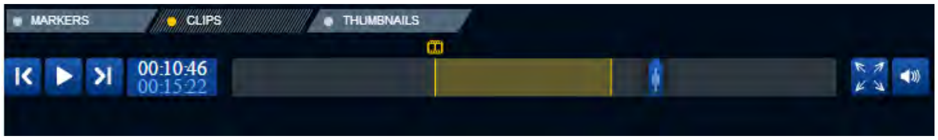
   The deleted marker no longer appears in the Markers list below the player.

Clips

A clip is a segment of a video or audio evidence file. When you create a clip, Evidence.com creates a new evidence file that you can use in the same way as other evidence.

Show and Hide Clips

You can control whether the scrub bar, located below the video image, shows yellow zones for each clip.

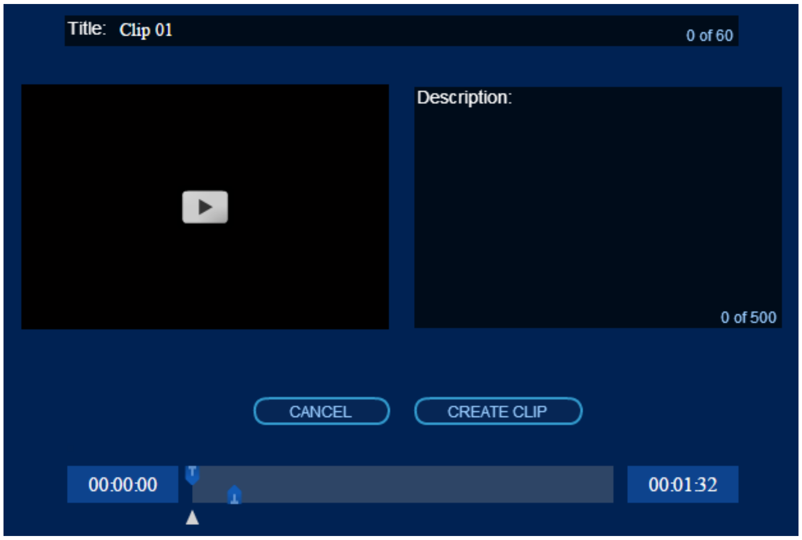


- To hide clip zones on the scrub bar, click ● CLIPS
- To show clip zones on the scrub bar, click ● CLIPS

Add Clip

1. On the View Evidence page, below the video or audio player, click **Add Clip**.

   The Create Clip dialog box appears over the player. On the scrub bar, two blue sliders appear. The time to the left of the scrub bar is the start time of the clip. The time to the right of the scrub bar is the end time of the clip.



Title: Clip 01 0 of 60

Description: 0 of 500

00:00:00 00:01:32

2. Use the two blue sliders to set the start and end of the clip.

   - To set the start of the clip, click and hold the left slider and then drag it to the time where you want the clip to start.

   - To set the end of the clip, click and hold the right slider and then drag it to the time where you want the clip to end.

3. On the video or audio player window, click ▶ (play) and review the clip.

4. If necessary, repeat steps 2 and 3 until the start and end of the clip are what you need.

5. In the **Title** box, type the title that you to give the clip.

6. In the **Description** box, type a useful description of what is shown in the clip.

7. Click **Create Clip**.

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

   Evidence.com generates a new video title, “Clip from [original evidence title]”. You can use an evidence search to find the video or audio clip.

View Clip

You can access clips from the View Evidence page of the evidence from which the clip was made.

1. On the View Evidence page, below the video or audio player and under Clips, find the clip that you want to view.

2. Click the clip title.

   The View Evidence page for the clip opens.

3. Use the features of the View Evidence page as needed.

Redacting a Single Video

For information about using the new redaction tools, see Video Evidence Redaction.

You can redact video evidence as needed, such as to ensure anonymity of persons in a video. Redaction never affects the original video. Instead, when you have finished redacting the video, Evidence.com generates a redacted version of the video.

The process of redaction involves placing one or more masks in the video. You can specify precisely which video frame a redaction mask applies to. The redaction mask types are the following:

- Vector — Redacts a portion of video frames, in a shape, color, and opacity that you specify.
- Blackout mask — Replaces video frames with a solid black frame.
- Filter mask — Obscures entire video frames with either a blur filter, an outline distortion filter, or a segmentation filter.
- Audio mask — Remove the audio from the frames that you apply the mask to.

For the video masks, you have the option of also redacting audio for the duration of the mask.

1. Play the video to about the first frame that you want to apply a new mask to and then click ⏸ (pause). You can pick the exact first frame more easily later.
2. From the tool bar, click ✂ (redact video).

   The Redaction Masks dialog box appears over the player.
3. Apply redaction masks to the video as needed. You can apply as many masks as required to ensure that the video is redacted to suit your needs. For information about specific mask types, see the following topics:
   - Add a Vector Mask
   - Add a Blackout Mask
   - Add a Filter Mask
   - Add an Audio Mask
4. Modify masks as needed. For information about specific actions, see the following topics:
   - Editing a Mask
   - Preview Mask
   - Rename a Mask
   - Deleting a Mask
5. On the Redaction Masks dialog box, click **Finish**.

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

   Evidence.com generates a new video title, “Redacted video of [original video title]”. You can use an evidence search to find the redacted video.

Add a Vector Mask

You can use a vector mask to redact parts of individual video frames. You can also redact the audio associated with those frames.

1. If the Redaction Masks dialog box is not open, from the tool bar on the player, click ✂ (redact video).

   The Redaction Masks dialog box appears over the player.

2. Click **New Mask**.

   The Add Mask dialog box appears.

3. Under **Mask Style**, click **Vector Mask**.

4. Under **Duration**, click **Find**.

   The Find First Frame Viewer shows the current frame.

5. Move the slider until the first frame that you want to redact appears.

6. Click **Confirm**.

   The Add Mask dialog box reappears.

7. Under **Color**, click **View**.

   The Opacity and Color Viewer shows a preview of the current frame and the selected vector details.

   By default, the mask is black and opaque (100% opacity).

8. If you want to change the mask color, click the desired color.

9. If you want the vector mask to be transparent, move the **Opacity** slider until the mask shown in the frame thumbnail under Mask Style.

10. Click **Confirm**.

    The Add Mask dialog box reappears.

11. Under **Vectors**, select the shape of the vector mask:

    - Elliptical
    - Rectangular

12. Choose whether you want to redact the area inside or the area outside of the vector mask:

    - Interior — Redact what is inside of the vector mask.
    - Inverted — Redact what is outside the vector mask.

13. Under **Audio**, select whether the audio associated with the redacted frames will be redacted, too. By default, audio is redacted. If you do not want to redact the audio, clear the “Redact associated audio” check box.

14. Click **Continue**.

    The video frame that you selected appears with the vector mask over it. Below the video is a frame bar that enables you to select other frames.

15. Apply the vector mask to frames as needed. The following table lists basic actions for applying a mask.

Basic Action	**Method**
Select a frame	You can do any of the following: • To move forward one frame, press **Right Arrow** or **D**. • To move backward one frame, press **Left Arrow** or **A**. • To jump to a specific frame, move the mouse pointer over the frame bar to the desired frame and click it.
Move the mask	1. Click and hold the mask, avoiding the handles at the corners. 2. Drag the mask to where you want it. 3. Release the mouse button.
Shape the mask	1. Click and hold a handle at one corner of the mask. 2. Drag the corner to where you want it. 3. Release the mouse button.
Apply the mask to the frame	Press **Down Arrow** or **S**.
Clear the mask from a frame	Press **Up Arrow** or **W**.

You can also use the following advanced actions.

Advanced Action	Method
Go to the next segment of video	Press **Shift + Right Arrow** or press **Shift + D**.
Go to the previous segment of video	Press **Shift + Left Arrow** or press **Shift + A**.
Apply the mask to a range of frames	If you do not need to move the mask from frame to frame, you can apply it to the range of frames: 1. Select the first frame in the range. 2. Apply the mask to the first frame. 3. Select the last frame in the range. 4. Apply the mask to the last frame. After you finish applying the mask, Evidence.com adds the mask to all frames in the range.

16. After you have applied to mask to the frames you want to redact, click **Confirm**.

    The Redaction Masks dialog box lists the vector mask that you created.

Add a Blackout Mask

1. If the Redaction Masks dialog box is not open, from the tool bar on the player, click ✂ (redact video).

   The Redaction Masks dialog box appears over the player.

2. Click **New Mask**.

   The Add Mask dialog box appears.

3. Under **Mask Style**, click **Blackout Mask**.

4. Under **Duration**, next to **Start Time**, click **Find**.

   The Find First Frame Viewer shows the current frame.

5. Move the slider until the first frame that you want to redact appears.

6. Click **Confirm**.

   The Add Mask dialog box reappears.

7. Under **Duration**, next to **End Time**, click **Find**.

   The Find Last Frame Viewer shows the current frame.

8. Move the slider until the last frame that you want to redact appears.

9. Click **Confirm**.

   The Add Mask dialog box reappears.

10. If you want to change the mask color, under **Color**, click the desired color.

11. Under **Audio**, select whether the audio associated with the redacted frames will be redacted, too. By default, audio is redacted. If you do not want to redact the audio, clear the “Redact associated audio” check box.

12. Click **Confirm**.

    The Redaction Masks dialog box lists the vector mask that you created.

Add a Filter Mask

1. If the Redaction Masks dialog box is not open, from the tool bar on the player, click ✂ (redact video).

   The Redaction Masks dialog box appears over the player.

2. Click **New Mask**.

   The Add Mask dialog box appears.

3. Under **Mask Style**, click **Filter Mask**.

4. Under **Duration**, next to **Start Time**, click **Find**.

   The Find First Frame Viewer shows the current frame.

5. Move the slider until the first frame that you want to redact appears.

6. Click **Confirm**.

   The Add Mask dialog box reappears.

7. Under **Duration**, next to **End Time**, click **Find**.

   The Find Last Frame Viewer shows the current frame.

8. Move the slider until the last frame that you want to redact appears.

9. Click **Confirm**.

   The Add Mask dialog box reappears.

10. Under **Filter Effect**, click the desired filter.

    - Blur
    - Outline Distortion
    - Segmentation

    To see an example of each filter type, hover the mouse pointer over the filter name.

11. Under **Audio**, select whether the audio associated with the redacted frames will be redacted, too. By default, audio is redacted. If you do not want to redact the audio, clear the “Redact associated audio” check box.

12. Click **Confirm**.

    The Redaction Masks dialog box lists the vector mask that you created.

Add an Audio Mask

1. If the Redaction Masks dialog box is not open, from the tool bar on the player, click ✂ (redact video).

   The Redaction Masks dialog box appears over the player.

2. Click **New Mask**.

   The Add Mask dialog box appears.

3. Under **Mask Style**, click **Audio Only**.

4. Under **Duration**, next to **Start Time**, click **Find**.

   The Find First Frame Viewer shows the current frame.

5. Move the slider until the first frame that you want to redact appears.

6. Click **Confirm**.

   The Add Mask dialog box reappears.

7. Under **Duration**, next to **End Time**, click **Find**.

   The Find Last Frame Viewer shows the current frame.

8. Move the slider until the last frame that you want to redact appears.

9. Click **Confirm**.

The Add Mask dialog box reappears.

10. Click **Confirm**.

    The Redaction Masks dialog box lists the vector mask that you created.

Editing a Mask

1. If the Redaction Masks dialog box is not open, from the tool bar on the player, click ✂ (redact video).

   Over the player, the Redaction Masks dialog box lists all the masks.

2. To the right of the mask that you want to edit, click **Edit**.

   The Edit Mask dialog box appears.

3. Change the mask as needed. For more information about options available for each type of mask, refer to the topic for adding that mask type:

   - Add a Vector Mask
   - Add a Blackout Mask
   - Add a Filter Mask
   - Add an Audio Mask

Preview Masks

1. If the Redaction Masks dialog box is not open, from the tool bar on the player, click ✂ (redact video).

   Over the player, the Redaction Masks dialog box lists all the masks.

2. Choose how you want to preview masks:

   - If you want to preview a single mask, next to the mask name, click **Preview**.
   - If you want to preview all masks, click **Preview All**.

   The player shows you the portions of the video affected the mask you selected or by all masks.

3. To end the preview, click ⏸ (pause).

   After you end the preview or after the preview completes, the Redaction Masks dialog box appears again.

Rename a Mask

1. If the Redaction Masks dialog box is not open, from the tool bar on the player, click ✂ (redact video).

   Over the player, the Redaction Masks dialog box lists all the masks.

2. Click the name of the mask that you want to rename.

3. In the **Mask Name** box, type the new name for the mask, and then click **OK**.

Deleting a Mask

1. If the Redaction Masks dialog box is not open, from the tool bar on the player, click ✂ (redact video).

   Over the player, the Redaction Masks dialog box lists all the masks.

2. For each mask that you want to delete, click ✕ (delete) and then click **Confirm**.

   The deleted masks no longer appear on the Redaction Masks dialog box.

Revision History

This section summarizes the changes to this guide, per each version of the guide. The revision table lists the versions in reverse order, so that you can more easily see the most recent changes to the guide.

Release Name and Document Revision	**Revision description**
August 2016 Rev. A	No changes were made to this guide in support of Evidence.com August 2016.
July 2016 Rev. A	Mask sizes for manual redactions enables agencies to more precisely redact small objects.
June 2016 Rev. A	• Axon Body 2 camera enhancements — Administrators can allow officers to enable/disable the indicator lights on their cameras. • CEW device setting update —The APPM setting now also controls the new Signal Performance Power Magazines (SPPMs). • Redaction enhancements — To simplify setting the start and end times of a redaction segment, the Start and End boxes support minutes and seconds. • Reports — Added the Sharing Audit Report that lists all user actions related to sharing evidence and cases, for a configurable date range.
May 2016 Rev. A	• In the Groups Administration section, information about the external ID of a group is available in the following procedures: o Search and View Groups o Edit Group Members, Monitors, and Other Settings • Minor changes to the View Case page are reflected in the View Case procedure, in addition to the Share a Case with Other Users in Your Agency, Share a Case by Download Link, and Share a Case with a Partner Agency procedures.
April 2016 Rev. A	• Accelerated video playback — Updated the Playing Video and Audio Evidence section with information about playing videos faster or slower. • Redaction enhancements — Updated the Video Evidence Redaction section to reflect changes to the video redaction tool suite. • View Evidence page enhancements — Updated the Working with Any Evidence section to reflect minor changes to the View Evidence page. • Reassignment of cases to groups — Updated the • Reassign Cases section to provide information about reassigning a case to a group.
March 2016 Rev. A	• Adding information about the simplified case acceptance changes, which enables an agency to receive shared cases from partner agencies without having to manually accept each shared case. For more information, see Receiving Shared Cases from Partner Agencies. • Added information about the Axon Capture mobile app. Axon Capture replaces the Evidence Mobile app.

Release Name and Document Revision	Revision description
February 2016 Rev. A	• The Supported Web Browsers section includes updated information about support for Internet Explorer and about disabling the Compatibility View setting. • The • Working with Image Evidence section includes new information about using the photo edit feature. • The Viewing Document Evidence section includes new information about viewing PDF document evidence in Evidence.com. • The Device Search — All Devices and My Devices section includes new information about how to search for unassigned devices.

Release 1.31 and Earlier Document Versions

The following table provides information about versions of this guide that describe Evidence.com release 1.31 and earlier.

Document version	Revision date	Revision description
23	1/26/2016	Release 1.31: • The Supported Web Browsers section includes updated information about end of support for Internet Explorer 8. • The Video Evidence Redaction section includes updated information about the following, new features available in manual redactions only: o Audio redaction o Blur level selection including blackout, configurable per redaction mask • The Axon Device Manager for Axon Body 2 Cameras section includes updated information about the general availability of the Axon Device Manager app in the Google Play store.

Document version	Revision date	Revision description
22	12/8/2015	Release 1.30: • Added information about end of support for Internet Explorer 8. • Updated the User Administration section with information about the following topics: o Simplified user states to Active and Inactive. o Ability to pre-provision Inactive users o Ability for administrators to control user account information and prohibit users from updating their own information. o Add User and Import Users feature updates. o Changes to deactivating users: reassigning evidence and devices when a user status is changed to Inactive is now optional rather than mandatory. • Updated the Media Player Controls section with information about the video quality selector feature. • Updated the Video Evidence Redaction section with information about the following topics: o Simplified redaction workflow, including a more visible Extract button. o Keyboard shortcuts for precise placement of redaction mask-segment handles. **3.** Added information about image tools that are available to agencies who request early access. See • Working with Image Evidence. • Added information about the new Axon device assignment app that is available to agencies who request early access. • Updated information about user audit trails, which are now available in CSV format in addition to PDF. See User Audit Trail. • Renamed the TASER Video Settings page to the Camera Settings page, with new settings for Axon Body 2. See Configure Camera Settings.
21	10/27/2015	• Updated information regarding adding and removing tags from evidence and cases. • Updated the Partner Agency Administration section, to reflect the changes the Partner Agencies page. • Added information about the audio and video file types supported by the Evidence.com media player. For more information, see Playing Video and Audio Evidence. • Revised and expanded the Case Management section. • Added the Partner Contact Search permission to Appendix A: Roles and Permissions. • Updated the Working with Markers and Clips section to reflect the name change of the Media Player tab to “Clips & Marker”. • Updated the Video Evidence Redaction section to reflect the name change of the Redactor tab to “Redactions”.
20.1	9/23/2015	Corrected the name of the assisted redaction feature.

Document version	Revision date	Revision description
20.0	9/22/2015	1.28 Release: • Added detailed information about using the new redaction tools, including manual redaction and assisted redaction. For more information, see Video Evidence Redaction. • Added the Supported Web Browsers section. • Added the Change Language section, which describes how users can select the language that Evidence.com uses when they sign in to your agency. • Revised the name of the "Fields & Retention" link on the Admin page to "Fields & Retention Categories". Affected sections include Evidence ID Validation and Categories and Evidence Retention Policies. • Revised information about permissions required to share evidence and cases, in Appendix A: Roles and Permissions. Specifically, sharing by download link and sharing with authenticated users in other agencies require separate permissions.
19.0	8/25/2015	1.27 Release: • Added information about the new media player. • Moved information about the traditional media player and its tools, including redaction, to an appendix. • Added information about evidence ID validation. • Updated CSV file format information for Import Groups, because files now require header rows. • Updated information about the Help section.
18.0	7/28/2015	1.26 Release: • Updated look and feel, to reflect the site refresh of all Evidence.com agencies. • Added the Import Groups, Members, and Monitors section. Other revisions: • Revised and expanded the Roles and Permissions section, including the new Appendix: Roles and Permissions. • Revised and expanded the Categories and Evidence Retention Policies section. • Revised and expanded the Evidence Management section.
17.0	6/23/15	1.25 Release: • Added the Groups Administration section • Updated information about search page names and behavior • Updated the User Administration section

Document version	**Revision date**	**Revision description**
16.0	5/26/15	1.22 Release: • Sharing with partner agencies is limited to one agency at a time • Password Reset is available on user search results page • Bulk video redaction, additional options 1.23 Release: • Partner agency setup changes • Reporting interface changes 1.24 Release: • Menu bar and other navigational changes • Dashboard changes • User Summary report support for single user reports • Evidence Search "View All" button removed • Bulk Evidence Sharing by unauthenticated download link • Case Creation support for adding evidence with the same ID • Case Invite page added for management of case invitations from partner agencies • Reporting support for Internet Explorer
15.0	2/20/15	1.21 Release: Case Sharing Enhancements, Bulk Over-Redaction, Clip & Redaction enhancements: backend processing, Tagged with AXONClip or AXONRedact, More detailed audit logs; Bulk download can exceed 4.2GB for zip files, Reports Enhancements
14.0	1/12/2015	1.20 Release: Active directory beta, clips and redacted files will now be created as new, separate pieces of evidence.
13.0	11/11/2014	1.19 Release: Updated Interagency Case Sharing, user reporting, bulk download to ISO file, extend retention duration without changing category, agency admin audit log
12.0	10/7/2014	Updated content based on 1.17 and 1.18 release: External case sharing, bulk download, IP whitelisting, expire all passwords, Reporting service, and change username.
11.0	11/4/2013	Updated content based on the Evidence.com 1.16 release
10.0	1/23/2013	Updated Settings Options, Categories & Retention, Devices Menu Options and screenshots based on the Evidence.com 1.15 release.
9.0	8/2/2012	Updated Settings Options, Import Evidence, Help Center topics and all relevant screenshots, and added a topic on Search based on the Evidence.com 1.14 release.
8.0	5/1/2012	Updated content and screenshots based on the Evidence.com 1.13 release Created a separate AXON Pro ETM Setup Guide and removed that content from this document.
7.0	3/8/2012	Updated content and screenshots based on the Evidence.com 1.12 release.
6.0	11/7/2011	Updated content and screenshots based on the Evidence.com 1.11 release.
5.0	8/17/2011	Updated content and screenshots based on the Evidence.com 1.10 release Merged content from the Quick Start Guide.

Document version	**Revision date**	**Revision description**
4.0	4/15/2011	Functionality test steps added.
3.0	4/12/2011	Installing ETM instructions added.
2.0	3/16/2011	Updated document for flow, format and content.
1.0	3/14/2011	Initial Document.