Getting Started with FileSworn

A practical guide to uploading, sharing, and tracking evidence.

1. Your Account and Dashboard

Creating Your Account

FileSworn supports four sign-in methods. Choose whichever is most convenient for your organization:

- **Email and password** - traditional login with a strong password
- **Magic link** - a one-time sign-in link sent to your email
- **Google OAuth** - sign in with your Google account
- **Microsoft OAuth** - sign in with your Microsoft/Azure AD account

Dashboard Layout

After signing in you land on the main dashboard. The left sidebar contains navigation links:

- **Evidence** - your uploaded files and cases
- **Shared Links** - active and expired share links
- **Productions** - discovery production tracking (Professional and above)
- **Settings** - account, billing, and notification preferences

At the top of the Evidence view, three stat cards show **Total Files**, **Active Shares**, and **Views Today**. Below them is a drag-and-drop upload area, a Cases section for organizing files by matter, and a searchable file list with filters for type, time, status, and mode.

Storage Tiers

Feature	Essential (Free)	Professional	Enterprise
Price	$0/mo	$149/mo	$499/mo
Storage	200 MB	50 GB	500 GB
Cases	3	Unlimited	Unlimited
Files	10	Unlimited	Unlimited
Productions	--	Yes	Yes
Certificates	--	FRE 902(13)	FRE 902(13)

2. Uploading and Organizing Evidence

Upload Process

Drag files onto the upload area or click to browse. FileSworn accepts images, video, audio, and PDF documents. During upload, a SHA-256 hash is computed automatically. This hash is the cryptographic fingerprint that proves the file has not been altered since the moment of upload.

Storage Modes

- **Temporary access** - the file auto-expires after a set period (24 hours, 7 days, 30 days, or a custom date). Use this for time-sensitive deliveries where the recipient should not retain permanent access.
- **Preserved evidence** - the file is stored permanently and supports litigation hold. Use this for evidence that must remain available for the duration of a matter.

Cases and Matters

Group related files under a Case. Each case has its own file list, and files within a case can be assigned Bates numbers. Bates numbering is auto-assigned per case and locked once set, so the numbering sequence is preserved for production records.

Tags and Search

Apply tags to files for quick categorization (e.g., "deposition", "surveillance", "medical"). The search bar and filter dropdowns let you narrow results by file type, upload time, status, and mode.

3. Sharing Evidence Securely

Creating Share Links

Select a file and click Share. Configure the link with an expiration date and optional view limit. Each share link generates a unique token. You can create multiple links for the same file with different settings. For batch sharing, send to multiple recipients at once. Each gets a unique link with their own watermark, so if a leak occurs the watermark identifies the specific recipient.

Recipient Verification and Watermark Levels

When a recipient opens a share link, they must verify their email address before viewing. This email is embedded in the viewer identity watermark. Choose the watermark detail level when creating the link:

- **Standard** - viewer email address
- **Detailed** - viewer email address and timestamp
- **Full** - viewer email address, timestamp, and IP hash

What the Recipient Sees

After verification, the recipient views the file in a full-screen watermarked viewer on a dark background. Every access event is recorded with timestamp, IP address, browser details, and the viewer's verified email.

Watermark Capabilities

What it does: embeds a visible identity overlay on every frame during viewing, provides attribution evidence linking a viewer to shared content, and records each session in the access audit trail. **What it does not do:** it does not prevent screen capture, does not embed invisible or steganographic data, and does not guarantee identification in all leak scenarios.

4. Monitoring Access

Access Audit Trail

Every time a recipient views a shared file, FileSworn records the event. The activity panel for each file shows a chronological list of access events with the following details:

- Viewer email address (verified at the gate)
- Timestamp of access
- Device and browser information
- IP address

Downloadable PDF Receipts

Each view event can be exported as a PDF receipt. These receipts are useful for court filings where you need to demonstrate that a specific person accessed specific evidence at a specific time.

Access Notification Emails

FileSworn sends email notifications when recipients view your shared files. Essential (free) accounts receive up to 10 notifications per month. Professional and Enterprise accounts receive unlimited notifications.

5. Certificates and Discovery Productions

FRE 902(13) Certificates

Professional and Enterprise accounts can generate Federal Rules of Evidence Rule 902(13) certificates. These self-authenticating certificates document the integrity of digital evidence and are designed to satisfy the requirements for admission without extrinsic evidence of authenticity.

Each certificate includes:

- **File identification** - file ID, original filename, MIME type
- **SHA-256 hash** - the cryptographic fingerprint computed at upload
- **Upload record** - timestamp and uploader identity
- **Access audit trail** - summary of all recorded view events
- **Viewer Attribution Methodology (Section 5)** - a four-step process: (1) recipient email verification at the gate, (2) identity watermark rendered in real time during viewing, (3) watermark persistence for the duration of the session, (4) log correlation linking the verified identity to each access event. This section is included only when at least one view has been recorded.
- **NTP Timestamp Authority** - clock synchronization reference
- **Independent Verification** - instructions for verifying the SHA-256 hash using sha256sum (Linux/macOS) or certutil (Windows)
- **Declaration under 28 U.S.C. 1746** - the legal attestation

Discovery Production Tracking

Professional and Enterprise accounts can use production tracking to document the handoff of evidence to opposing counsel or other parties. This feature is not e-discovery software. It tracks the moment of production and creates a record of delivery.

The production workflow:

- Select files and assign a production number
- Bates-numbered production logs with SHA-256 hashes are generated
- Send via watermarked share links with per-recipient identity tracking
- Status updates automatically: Draft to Sent (when share links are created), Sent to Confirmed (when the recipient accesses the files)
- Download a production log PDF summarizing the entire handoff

6. Quick Reference

Key Actions

Action	How
Upload a file	Drag onto dashboard or click Upload
Create a case	Evidence tab > New Case
Share a file	Select file > Share > set expiration and watermark level
View access history	Select file > Activity panel
Generate certificate	Select file > Certificate (Professional+)
Create production	Productions tab > New Production (Professional+)
Set litigation hold	Select preserved evidence file > toggle Litigation Hold
Export PDF receipt	Activity panel > click view event > Download Receipt

Contact and Resources

- **Email:** anthony@filesworn.com
- **Demo certificate:** filesworn.com/demo/certificate
- **Schedule a demo:** calendly.com/anthony-kulick/filesworn-demo
- **Resources:** filesworn.com/resources

Thank you for choosing FileSworn. If you have questions or need help getting started, reach out to us at anthony@filesworn.com.