

The Evidence Custodian Handbook

A walkthrough of the account, evidence, Section 63 certification, and enterprise features — with the spots people tend to get stuck, called out as they come up.

RECENTLY ADDED

Every screen shown here reflects the current build: two-factor authentication (TOTP, no external service), Cloudflare Turnstile CAPTCHA (with an automatic fallback to a math question until it's configured), and a contextual ? next to fields whose purpose, format, or consequence isn't obvious — hover it, or tap it on a touch screen. Several of the screenshots below show one open.

CONTENTS

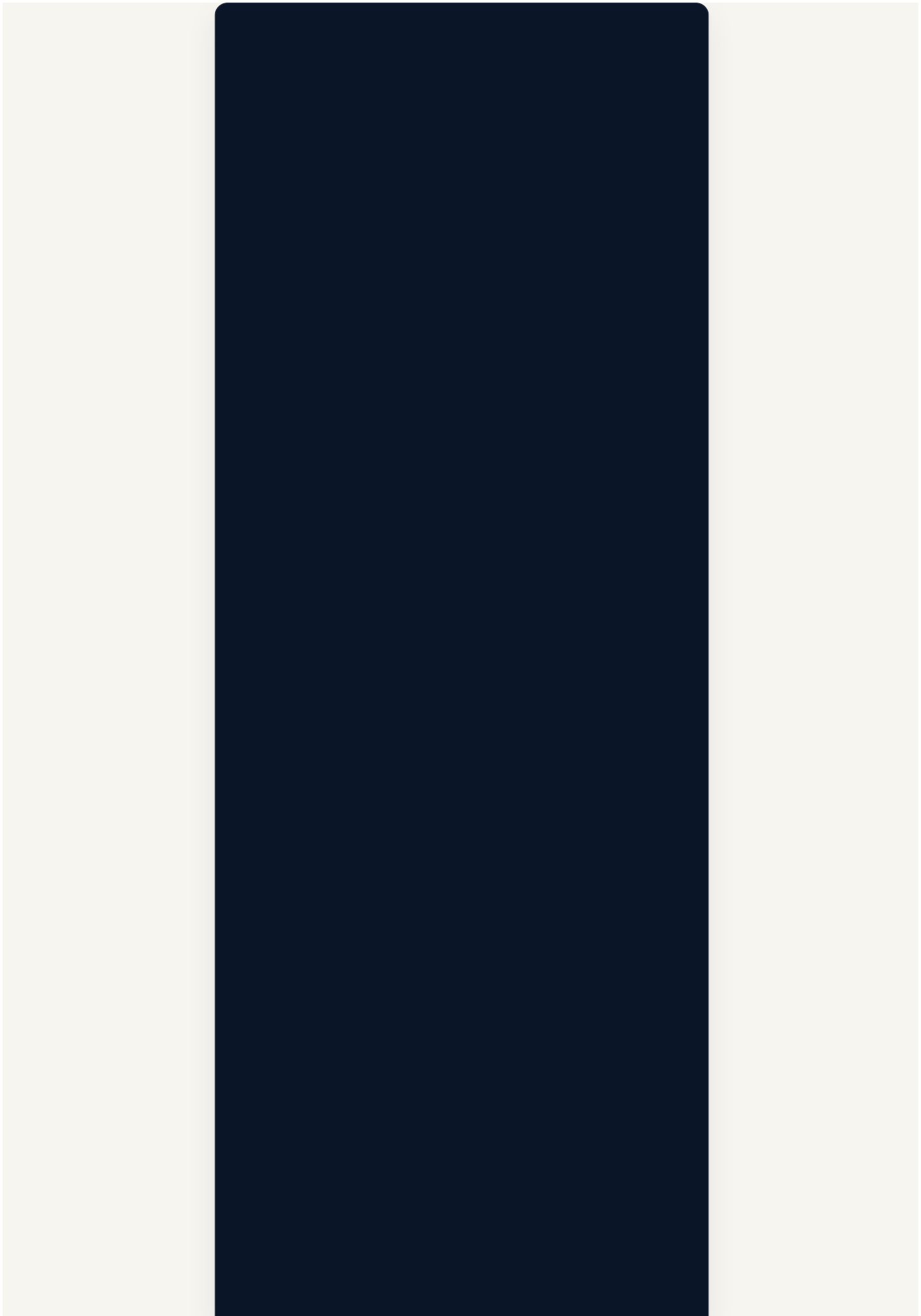
01	Getting started	02	Securing your account
03	Uploading evidence	04	Certifying under Section 63
05	Enterprise features	06	Billing & plans
?	Common points of confusion		

01 Getting started

Creating an account, and the two ways to arrive at the sign-in screen.

The landing page

Both the login and registration forms live on the home page as tabs, so a first-time visitor never has to pick the "right" link.



Section 63 BSA Compliant

Secure Your Digital Evidence for Indian Courts

Generate legally admissible certificates for digital evidence as per Section 63 of Bharatiya Sakshya Adhiniyam (BSA), 2023. Trusted by lawyers, law enforcement, and forensic professionals across India.

- ✓ SHA-256 Hash Verification
- ✓ Statutory Part A + Part B Certification
- ✓ Metadata Extraction
- ✓ Court-Ready PDFs

Start Free Trial

See How It Works

POWERFUL FEATURES

Everything You Need for Digital Evidence

Comprehensive tools designed specifically for Indian legal requirements and digital forensics standards.



Cryptographic Hashing

SHA-256 hash generation ensures evidence integrity, verified again at every stage. Any tampering becomes detectable and documented.



Statutory Two-Party Certification

Part A (owner/custodian declaration) and Part B (forensic expert declaration), generated to match the BSA 2023 Schedule wording - not a generic hash report.



Bulk Upload & Certification Groups

Process an entire case's worth of files at once, then split into separate certification groups when evidence comes from different devices or declarants.



Immutable, Versioned Certificates

Once issued and locked, a certificate cannot be silently edited. Corrections create a new version; the original is preserved, not overwritten.



Independent Verification Portal

Anyone holding a certificate can verify it against the original evidence directly, without relying on the PDF alone.



Metadata Extraction

Automatic extraction of EXIF data, GPS coordinates, device info, and creation timestamps from media files.



Complete Audit Trail

Every stage of a certificate's lifecycle - from upload through signing to issuance - is timestamped and traceable, tamper-evident by design.



Video, Image & Document Support

Video, images (including RAW camera formats), and supporting documents like PDFs and Office files - not just phone photos and screenshots.

SIMPLE PROCESS

How It Works

A guided path from upload to a court-ready statutory certificate.

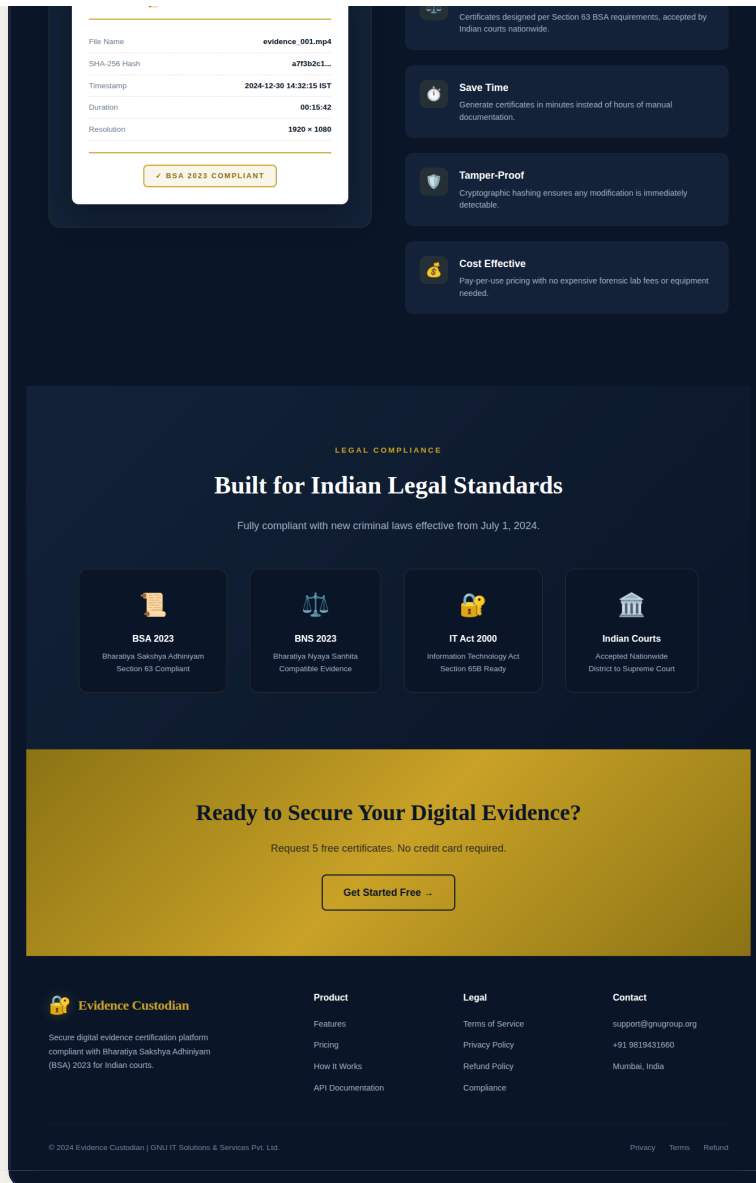


WHY CHOOSE US

Benefits for Legal Professionals

Section 63 BSA Certificate

Court Admissibility



The landing page. Login and Register are tabs on the same card, not separate pages.

Registering

Only name, email, and password are required. Organization and GSTIN are both optional — GSTIN only matters if you'll need GST invoices later, and it has a strict 15-character format the form checks before it lets you submit.

Evidence Custodian
Create Account
Start securing your digital evidence today

Get 5 free certificates upon registration

Full Name * Organization ?
Your Name Company/Firm (option)

Email Address *
you@example.com
This will be your login email

GSTIN (Optional) ?
ZSAAAA0000A1Z5

For GST invoice generation
Password * Confirm Password *
Min 8 characters Repeat password

Security Check: 30 - 9 + 7
Enter the answer

☐ I agree to the Terms of Service and Privacy Policy

Create Account

Already have an account?
Sign in here
Back to Home

The full registration form.

Evidence Custodian
Create Account
Start securing your digital evidence today

Get 5 free certificates upon registration

Full Name * Organization ?
Your Name Company/Firm (option)

Email Address *
you@example.com
This will be your login email

GSTIN (Optional) ?
ZSAAAA0000A1Z5

For GST invoice generation
Password * Confirm Password *
Min 8 characters Repeat password

Security Check: 30 - 9 + 7
Enter the answer

☐ I agree to the Terms of Service and Privacy Policy

Create Account

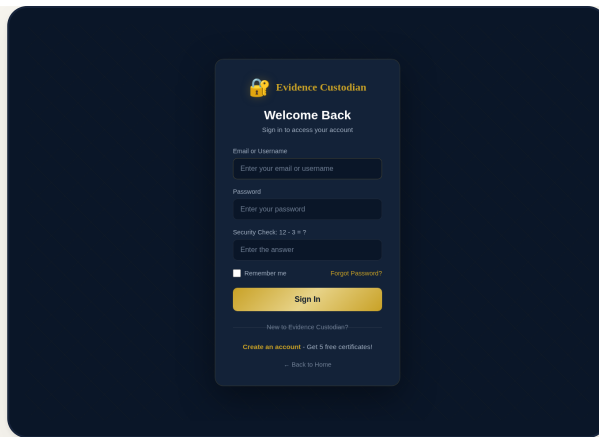
Already have an account?
Sign in here
Back to Home

Enter the only if you need GST number for your purchase. Format: 15 characters. 2-digit state code, 10-character PAN, 1-digit entity code, the letter Z, then a checksum character (e.g. ZSAAAA0000A1Z5). Lower & upper character, & body character case will be rejected at sign-up.

Tapping the ? next to GSTIN spells out the exact format – state code, PAN, entity code, checksum – so a typo gets caught before submission, not after.

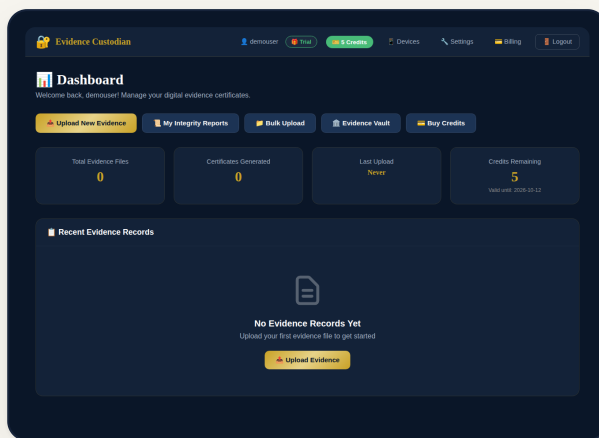
Signing in

The field above the password takes **either** your email address or your username — whichever you registered with is what got stored, and the sign-in form no longer insists on email formatting to accept it. If you forget which one you used, either will work as long as it's correct.



The identifier field reads Email or Username and accepts either.

Forgotten your password entirely? The link below the form sends a reset email to the address on file.



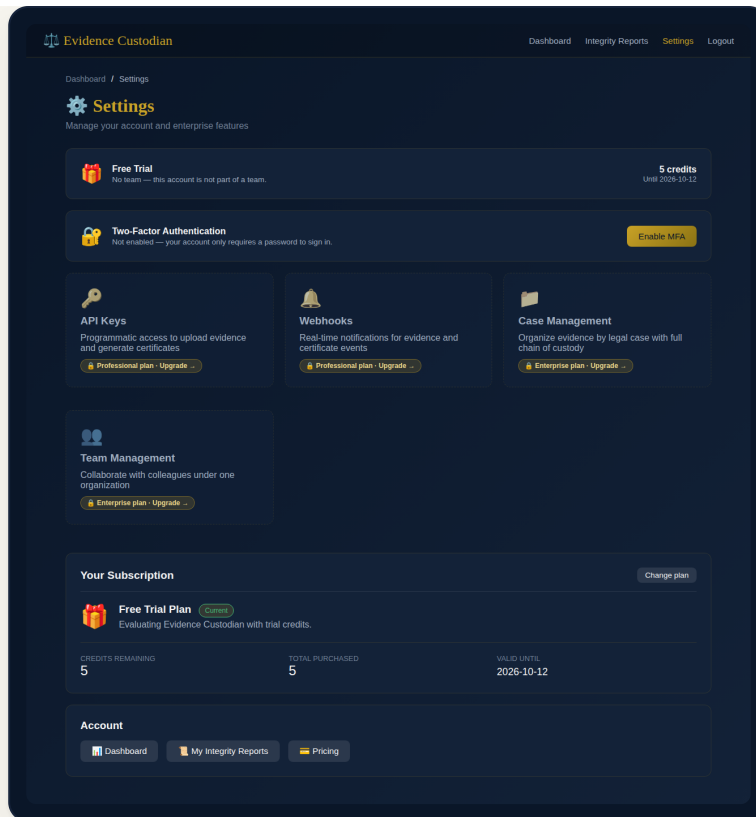
Password reset asks only for the email on the account.

02 Securing your account

Two-factor authentication is optional, self-contained (no external service to configure), and lives entirely under Settings.

Before you turn it on

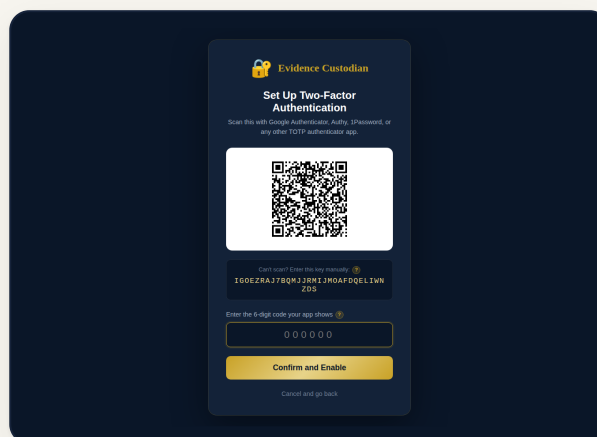
The Settings page shows a Two-Factor Authentication card whether or not it's enabled yet — this is what it looks like before you have.



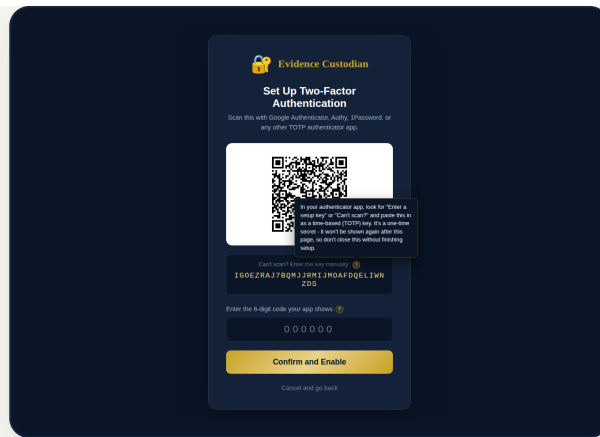
Settings, before enabling two-factor authentication.

Enrolling an authenticator app

Scan the QR code with Google Authenticator, Authy, 1Password, or any other TOTP app. Can't scan it — a desktop browser, say — use the manual key underneath instead.



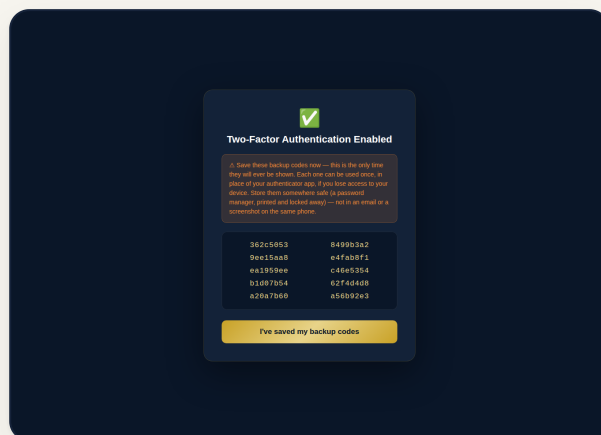
Scan, or copy the manual key by hand.



The manual key's tip explains where to paste it, and warns it's shown only this once.

SAVE THESE BEFORE YOU CLOSE THE PAGE

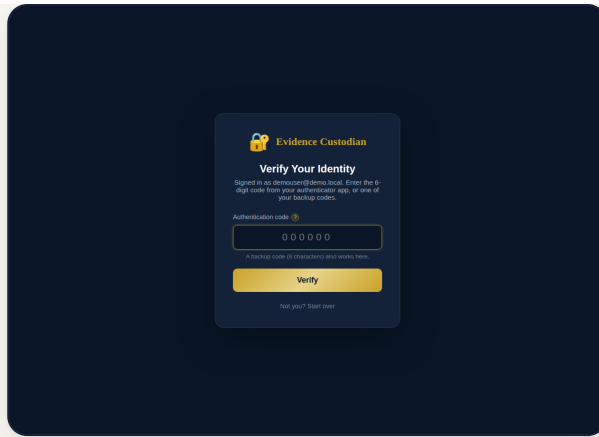
Confirming the code on this screen immediately shows ten backup codes — each usable once, in place of your authenticator app. This is the only time they're ever displayed. Store them somewhere durable (a password manager, a printed copy in a locked drawer) rather than a screenshot on the same phone that has the authenticator app.



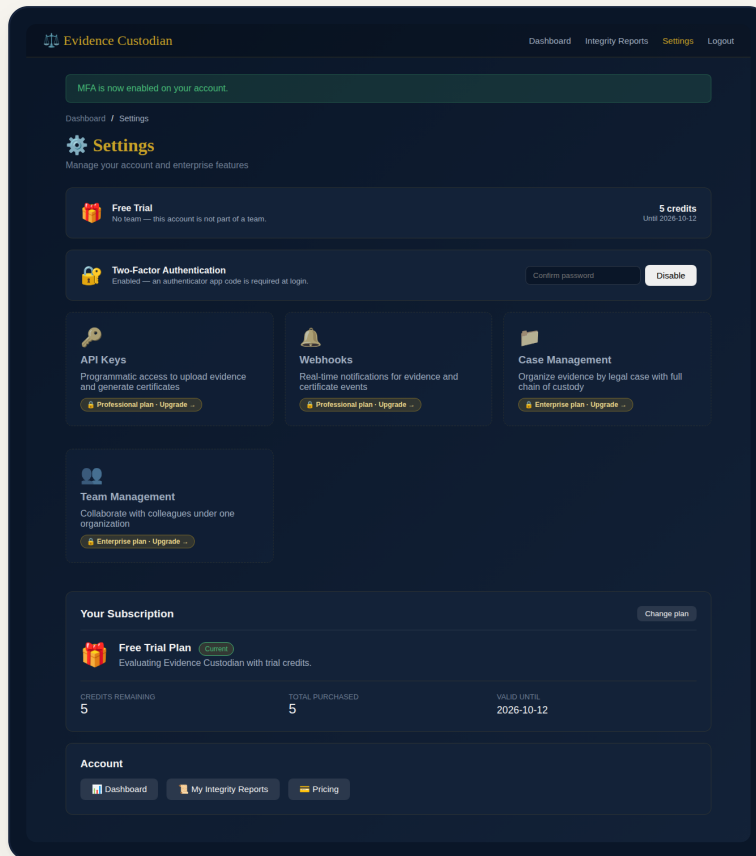
Ten single-use backup codes, shown exactly once.

Signing in afterward

Once MFA is on, a correct password no longer signs you in by itself — it hands off to this second screen first.



The authenticator code or a backup code both work here.



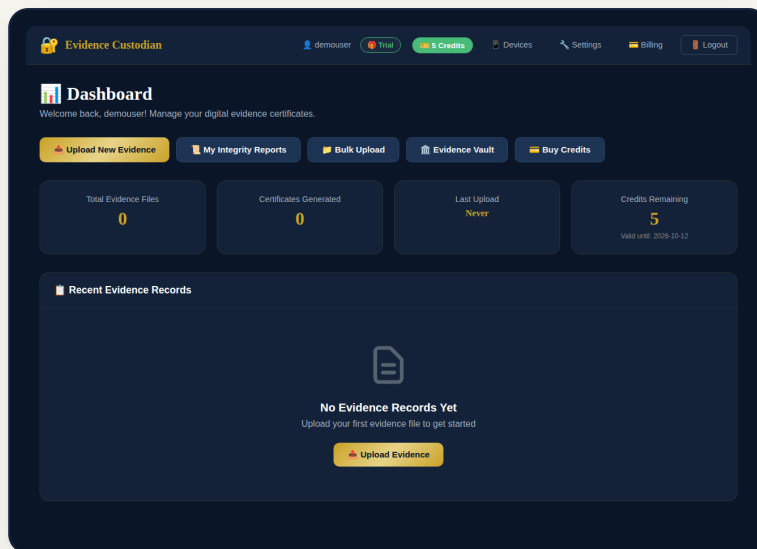
Settings afterward – disabling it back here asks for your password to confirm.

03 Uploading evidence

One file at a time, or up to a hundred at once — each gets its own certificate either way.

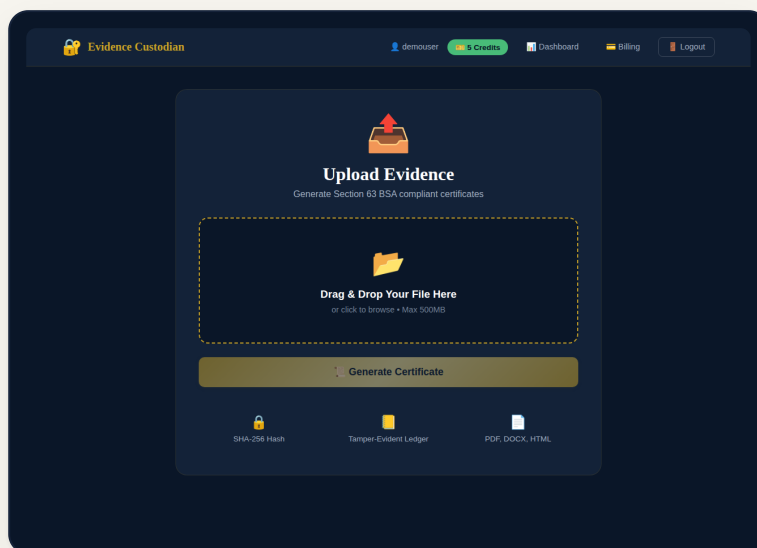
Your dashboard

The dashboard is where you land after signing in, and where every other feature is one click away.



The dashboard.

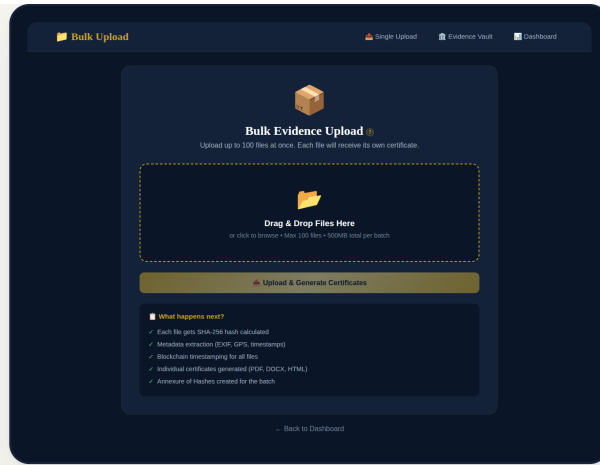
Single-file upload



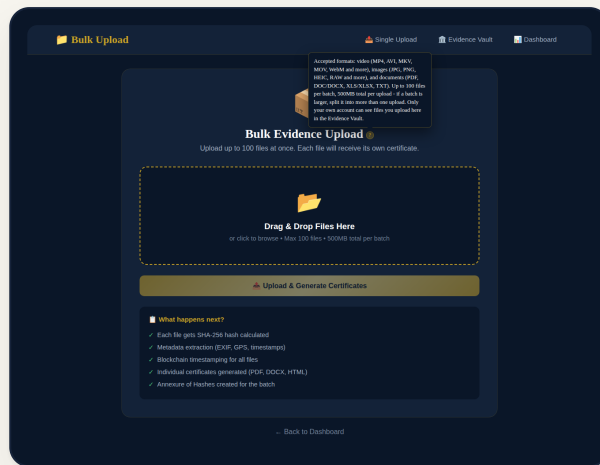
Single-file upload – the quickest path from file to certificate.

Bulk upload

Drag up to a hundred files at once. The limit that matters is 500MB for the *whole batch*, not per file — if a batch is bigger, split it into two uploads rather than trying to shrink individual files.



Drag files in, or click to browse.



The heading's tip lists accepted formats and clarifies the 500MB figure.

04 Certifying under Section 63

The statutory certificate under Section 63(4)(c) of the Bharatiya Sakshya Adhiniyam, 2023 — the most legally consequential forms in the product, and where the field-by-field hints (a permanent line of text under a field, not a hover tip) matter most.

Recording the original source

Before either declaration, the platform needs to know where the record originally came from — the phone, DVR, or cloud account, not the file you uploaded. Saved devices can be reused (and optionally shared with your team) so this doesn't get retyped every time.

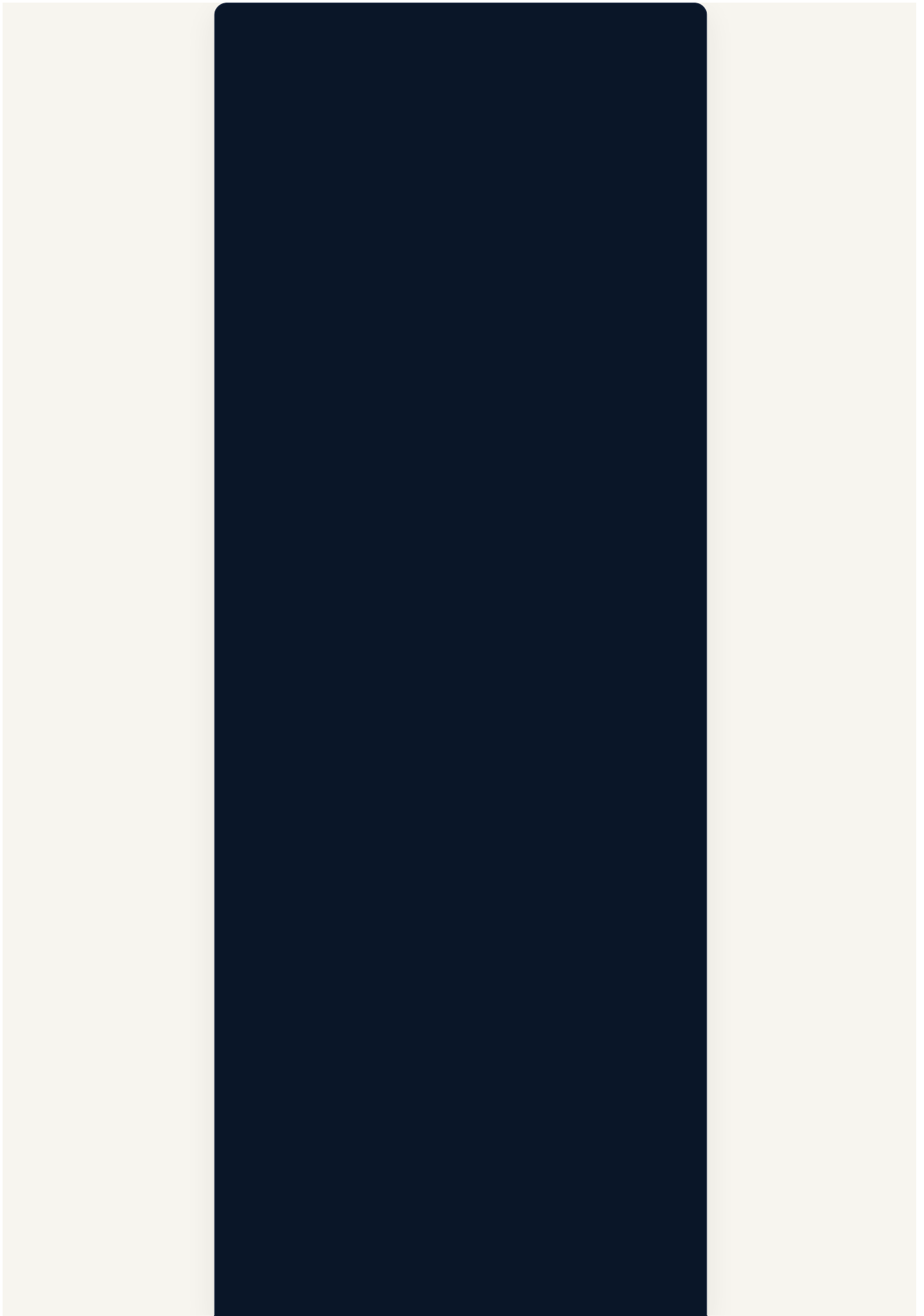
Original source particulars, with the extraction-method tip open.

Saving a device for reuse across future uploads.

Part A — the party's declaration

Completed by whoever had lawful control of the original device or account.

Every field below the source particulars carries its own hint line, and the declaration checklist and hash-algorithm choice each get a fuller explanation behind a ?.



Part A — Declaration by the Party

Certificate under Section 63(4)(c), Bharatiya Sakshya Adhiniyam, 2023

Part A must be completed by the person who had lawful control of the original device or account and direct knowledge of how the record was produced. Acting as a party's advocate is not, by itself, sufficient to sign Part A.

How would you like to sign?

Aadhaar eSign (recommended)

Recommended. Sign with your Aadhaar-linked OTP or biometric authentication — no printing, no scanning. An electronic signature under s.3A of the IT Act, 2008, issued through a licensed eSign Service Provider.

Not yet connected to an eSign provider. Use the form below for now.

Sign in this form

Type your name and affirm the declarations below. Recorded honestly as a typed name acknowledgement — not a signature within the meaning of IT Act s.5.

Print & sign by hand

Fill in the form, print it, sign it physically, and upload the scan. Recorded as a wet-ink signature — verifiable by inspection of the original.

Declarant

Full name *

Rajesh Kumar Sharma

Full legal name of the person declaring — e.g. **Rajesh Kumar Sharma**

Son/daughter/spouse of

Prescribed by the Schedule, not optional — e.g. **S/o Mohan Sharma**

Residential or employment address *

Residential OR employment address, as applicable — e.g. **12 Nariman Point, Mumbai 400021**

1. Identification of electronic record

Description of record

e.g. Photographs taken during site inspection

What the records are — e.g. **Photographs taken during site inspection**

File name(s)

IMG_2041-.jpg

One file per line, exactly as named when produced — e.g. **IMG_2041.jpg**

Relevant date or period

e.g. 15/08/2026 to 20/08/2026

The period the declaration covers — e.g. **15/08/2026 to 20/08/2026**

Case/reference number, if any

Your matter or court reference, if any — e.g. **CS123/2026**

2 & 3. Source and device particulars

These were recorded earlier and are shown for your confirmation. If anything is wrong, correct it before signing — particulars lock once Part A is signed.

Source type	Smartphone
Make and model	Samsung Galaxy S23
Colour	Phantom Black
Serial number	RZ8W10ABCDE

4. Manner in which the record was produced

Describe the collection, download, export, copying or extraction process, including date, time, the person performing it and tools used

How the record was obtained, including date, person and tool — e.g. **Exported over USB using Smart Switch 4.3.23 on 25/08/2026 by R. Sharma**

5. Declaration concerning statutory conditions ⓘ

Affirm each statement individually. They are deliberately not pre-selected — a pre-ticked declaration carries little weight under cross-examination.

I state that, during the relevant period:

- ☒ I had lawful control over the device or digital source identified above during the material period.
- ☒ The information was regularly created, stored or processed by the said device or digital source in the ordinary course of activity.
- ☒ The information contained in the electronic record was supplied to the device or digital source in the ordinary course of activities.
- ☒ The device or digital source was operating properly during the material period, or if not, any malfunction did not affect the accuracy or integrity of the electronic record.
- ☒ The electronic record produced is a true and accurate reproduction of the information from the said device or digital source.

My relationship with the source/device was

☒ Owned by me ☒ Maintained by me ☒ Managed by me ☒ Operated by me

If other, explain

SHA-256 is the platform default and what it used to calculate the values below. Keep it selected unless you have a specific reason to record a different algorithm (e.g. matching an existing case file that already used MD5(SHA-1)).

Hash algorithm used ⓘ

☒ SHA-256 (recommended) ☒ SHA-1 ☐ MD5 ☐ Other legally acceptable algorithm

These are the values this platform calculated when the files were received. Signing Part A adopts them. You are not asked to retype them — retyping 64 characters per file would only introduce error.

NO.	FILE	SHA-256 RECORDED BY THE PLATFORM
1	IMG_2041_.jpg	a1b2c34d5f6a1b2c34d5f6a1b2c34d5f6a1b2c34d5f6a1b2c34d5f6a1b2

The complete values also appear in the hash report enclosed as Annexure 1. If any value looks wrong, stop and raise it before signing.

Declaration and signature

I declare that the particulars stated above are true and correct to the best of my knowledge and belief.

How are you signing this declaration? *

☒ Type your name below. Recorded honestly as a typed name acknowledgement — not a signature within the meaning of IT Act s.5.
☐ Print this declaration, sign it by hand, then upload a scan or photo of the signed page.

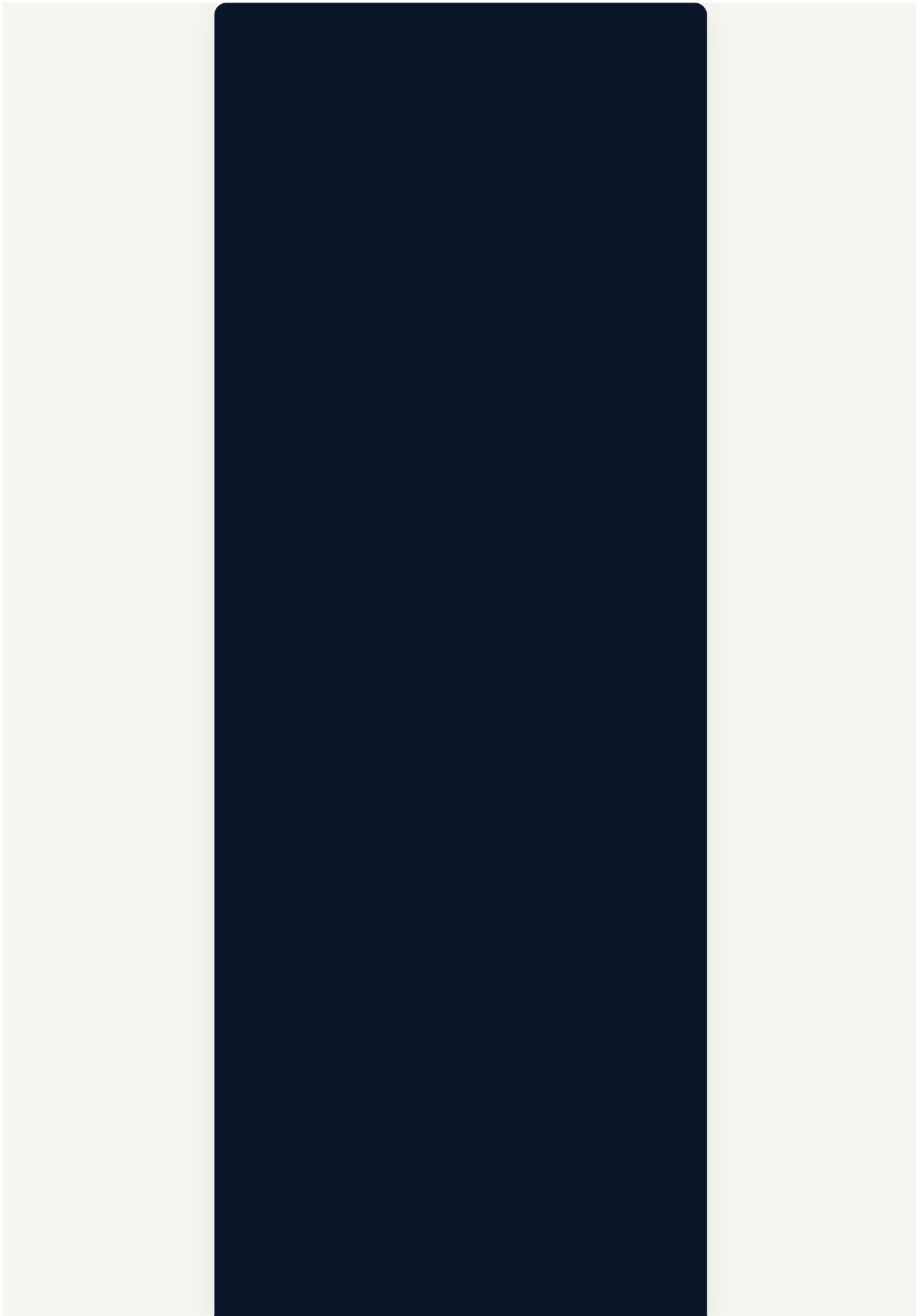
Name (as signed) *

The screenshot shows a digital form interface on a dark blue background. At the top, there is a text input field with a placeholder that says "Type your full name exactly as it appears above — e.g. Rajesh Kumar Sharma". Below this is a section titled "Capacity/relationship to the record" with a text input field containing "e.g. Owner of the device". Underneath, it says "Your relationship to the record — e.g. Owner of the device". The form then has three input fields: "Date (DD/MM/YYYY) *" with the value "03/09/2026", "Time (HH:MM:SS IST) *" with the value "14:30:00", and "Place *". At the bottom left, there is a yellow button labeled "Sign Part A" and a grey button labeled "Cancel". At the very bottom, in small text, it says "Once signed, the source particulars lock so the declaration keeps matching exactly what was attested."

Part A in full, with the hash-algorithm tip open over the declaration checklist.

Part B — the expert's declaration

A separate, independent hash calculation — the platform's own computed value is deliberately withheld on this form, since Part B only has evidentiary weight if it reflects a genuinely separate examination. The Section 79A status field is usually the one question people hesitate on.



Part B — Declaration by the Expert

Certificate under Section 63(4)(c), Bharatiya Sakshya Adhiniyam, 2023

Please calculate the hash yourself, using your own tools, and record what you found. The value computed by this platform is deliberately not shown on this form — Part B has evidentiary value only if it represents an independent examination.

How would you like to sign?

Class 3 DSC (USB token) (coming soon)

Recommended for forensic professionals holding their own token. A digital signature under IT Act s.36(5), applied via a local signing bridge you install once. The strongest form of signature available here. Not yet connected to a signing bridge provider.

Aadhaar eSign (coming soon)

Alternative for certified institutional experts without a personal token. An electronic signature under s.3A, via a licensed eSign Service Provider. Not yet connected. Use the form below for now.

Print & sign by hand

Fill in the form, print it, sign it physically, and upload the scan. Recorded as a wet-ink signature — verifiable by inspection of the original.

Or complete the declaration below and affirm by typing your name — recorded honestly as a typed-name acknowledgement, not a signature within the meaning of IT Act s.5.

Expert

Full name *

Rajesh Kumar Sharma

Expert's full legal name — e.g. Dr Priya Nair

Son/daughter/spouse of

Prescribed by the Schedule, not optional — e.g. Shri Mohan Sharma

Residential or employment address *

Residential OR employment address, as applicable — e.g. 12 Nariman Point, Mumbai 400021

Designation/qualification *

e.g. Cyber Forensic Analyst, M.Tech (CS), CFI

Role or professional title — e.g. Cyber Forensic Analyst

Organisation, if applicable

Employer, or state independent practice — e.g. Independent practice

Section 79A notification reference, if you are a notified Examiner

Optional. Following the Supreme Court's 2026 ruling, experts are not confined to notified Examiners, but the court must be satisfied of your expertise — so state your qualifications fully above.

1. Electronic record examined

Description of record/output

File name(s)

IMG_2841.jpg

One file per line, exactly as named when produced — e.g. IMG_2041.jpg

Case/reference number

2 & 3. Source and particulars

Record the source as you identified it. Part A's entries are not copied here.

Source from which the record was obtained

Select...

Make and model, colour, serial number, IMEI/UN/UID/MAC/Cloud ID, other identifying information

4. Hash verification

Hash algorithm used

☒ SHA-256

(recommended)

☐ SHA-1☐ MD5☐ Other legally

acceptable

Enter the value you calculated for each file. The platform's own values are deliberately not shown: Part B has evidentiary weight only if it records an independent calculation.

1: IMG_2041.jpg *

64 hexadecimal characters

Date and time of hash calculation *

DDMMYYYY HH:MM:SS IST

When you personally ran the hash tool - not when the record was created — e.g. 25/08/2026 15:42:00 IST

Tool/software used, with version *

e.g. sha256sum (GNU coreutils 9.4); Autopsy 4.21

Tool and version used for your calculation — e.g. sha256sum (GNU coreutils 9.4)

Relevant technical observations or limitations

State 'None' if there are none

Any limitations on your examination — e.g. None, or 'Original device not examined'

What you examined

Object personally examined *

Select...

State what you actually inspected — not what it came from.

Forensic image ID, if you examined an image

e.g. FI-2026-0091

Evidence

Choose "Yes" only if you're formally notified as an Examiner of Electronic Evidence under Section 79A. If you aren't, or aren't sure, choose "Not claimed" - following the Supreme Court's 2026 ruling, unnotified experts can still give this opinion, but you'll need to state your qualifications and experience below so the court can assess your expertise.

Your qualification

Section 79A Examiner status *

Select...

Where Section 79A status is not claimed, these are required so the court can assess demonstrable special skill.

Relevant certifications

e.g. CFI, EnCE

Relevant experience

e.g. 8 months as portable device forensics

Area of special skill
e.g. Mobile acquisition and hash verification

Supporting credential document
e.g. CV_PNair_2026.pdf

Credential document SHA-256

Declaration and signature

I confirm that the enclosed hash report records the hash value or values calculated for the electronic record identified above, and that the particulars recorded in this Part are true and correct to the best of my knowledge and belief.

How are you signing this declaration? *

Type your name below. Recorded honestly as a typed name, acknowledgement — not a signature within the meaning of IT Act s.5. Press the declaration, sign it by hand, then upload a scan or photo of the signed page.

Name (as signed) *

Type your full name exactly as it appears above — e.g. Rajesh Kumar Sharma

Date (DD/MM/YYYY) * Time (HH:MM:SS IST) * Place *

03/09/2026 14:30:00

Sign Part B

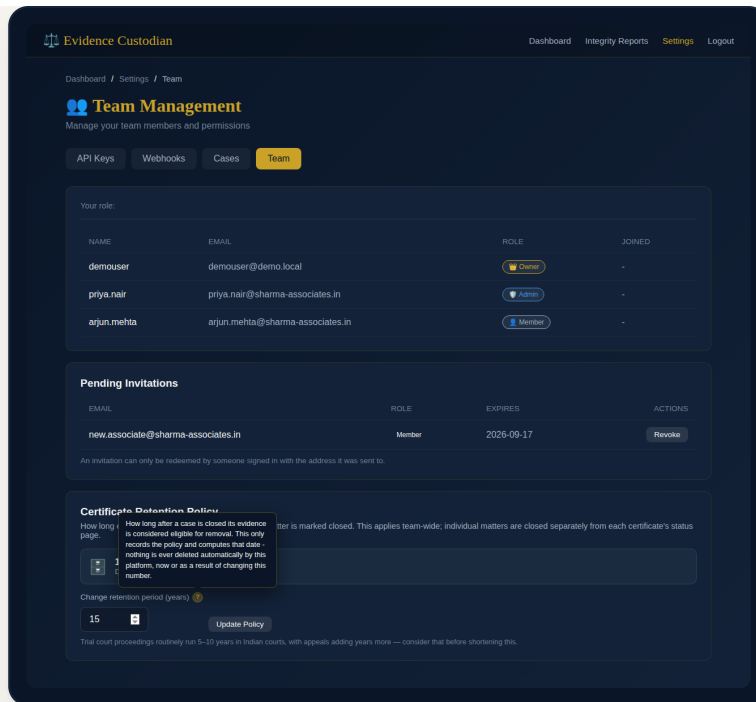
Part B, with the Section 79A status tip open – choosing "Not claimed" is fine and still lets the declaration proceed.

05 Enterprise features

Teams, API access, webhooks, and case organization — available on the Enterprise plan.

Team & retention policy

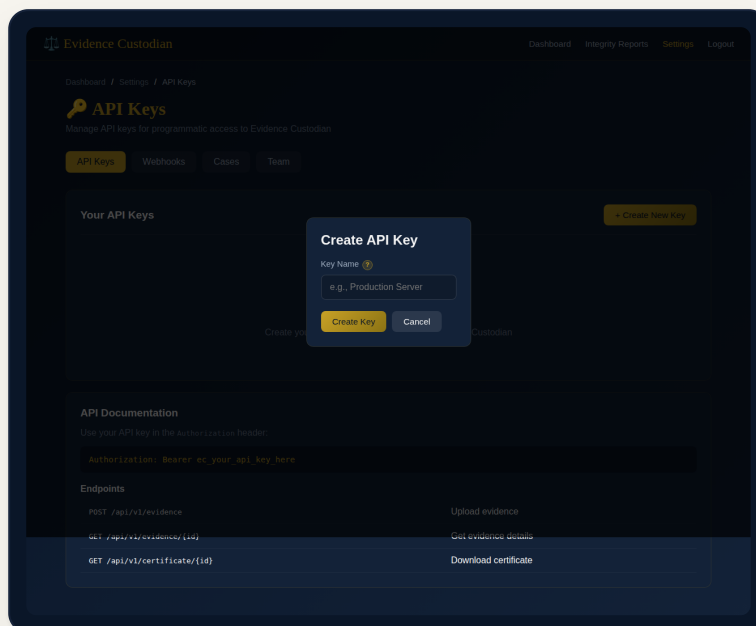
Inviting a colleague sets their role at the same time. The retention policy further down the same page is a records-keeping setting only — it computes a date, nothing more; the platform never deletes evidence on its own.



Team roster and retention policy, with the retention tip open.

API keys

A key is shown in full exactly once, right after creation — have somewhere to paste it ready before you click Create.

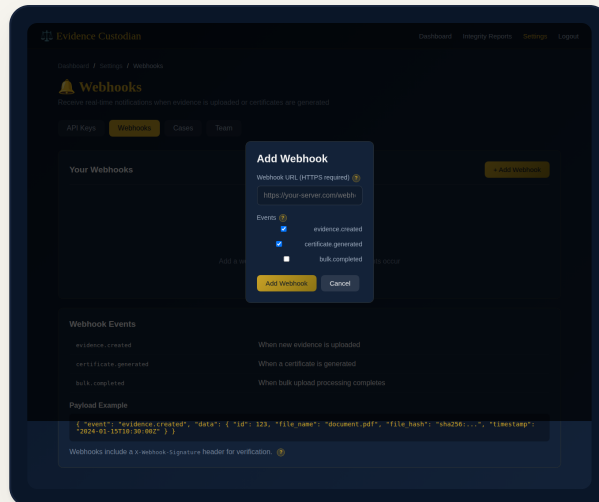


Naming a new key. The name is just a label – it doesn't affect what the key can do.

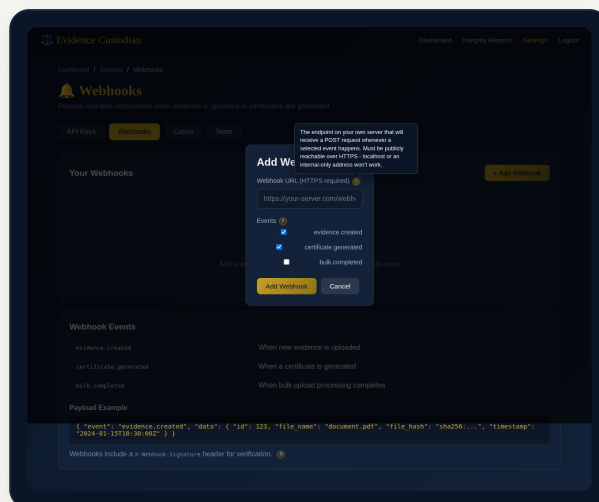
Webhooks

Choose the events that should notify your own server, and over HTTPS only. The signing secret used to verify X-Webhook-Signature is shown once, in

full, right after you add the webhook — if it wasn't saved, deleting and re-adding the webhook is the only way to get a fresh one.



Adding a webhook, with the URL tip open.



The signature scheme, spelled out where it's actually used.

Cases

A case is a folder, not a certificate — it groups evidence records under one chain of custody. Only the title is required at creation; everything else can be filled in as it becomes known.

Evidence Custodian

A case is a container you attach evidence records to, so everything relating to one matter stays grouped under one chain of custody instead of scattered across separate uploads. Only Case Title is required - fill in the rest as it becomes known.

Dashboard / Settings

Create New Case

Case Title *

e.g., Smith vs. Jones Property Dispute

Case Number

e.g., CIV/2024/001234

Court

e.g., Delhi High Court

Client Name

Client or party name

Description

Brief description of the case...

Create Case

Cancel

Creating a case, with the heading's tip explaining what a case actually does.

06 Billing & plans

Pricing is self-serve; Enterprise is a conversation.

Evidence Custodian

Upload

Dashboard

Logout

Choose Your Plan

Select the perfect plan for your digital evidence certification needs. All plans include blockchain timestamping.

Basic

For individual lawyers and small cases

₹499

100 Credits

100 Credits (₹100) + ₹100

✓ 50 Evidence Certifications

✓ Valid for 12 months

✓ PDF, DOCX, HTML Certificates

✓ Blockchain Timestamping

✓ SHA-256 Hash Verification

✓ Email Support

Get Started

Professional

For law firms and frequent users

₹1499

200 Credits

200 Credits (₹200) + ₹1299

✓ 200 Evidence Certifications

✓ Valid for 12 months

✓ All Certificate Formats

✓ Blockchain Timestamping

✓ Bulk Processing (100 files)

✓ Evidence Vault with CoC

✓ Priority Support

Get Started

Enterprise

For large organizations

Custom Pricing

Custom pricing for quote

✓ Unlimited Certifications

✓ All Features Included

✓ API Access

✓ Custom Integration

✓ Dedicated Account Manager

✓ SLA Guarantee

Contact Sales

Or Buy Credit Packs

All credits valid for 12 months from purchase date

10 Credits

₹149

GST + ₹10%

Buy Now

25 Credits

₹299

GST + ₹10%

Buy Now

50 Credits

₹499

GST + ₹10%

Buy Now

100 Credits

₹999

GST + ₹10%

Buy Now

Secure payments via Razorpay — UPI, Cards, Netbanking & Wallets

[Back to Upload](#)

Plans and pay-per-use packs.

The screenshot shows a dark-themed web interface for 'Evidence Custodian'. At the top, it says 'Evidence Custodian' with a logo. Below that is a header for 'Enterprise Plan' with the subtitle 'Custom solutions for large organizations and law firms'. The main content is divided into two columns. The left column, titled 'Enterprise Features', lists various capabilities with green checkmarks: Unlimited Evidence Certifications, All Certificate Formats, Blockchain Timestamping, Bulk Processing (Unlimited), Evidence Vault with CoC, API Access, Custom Integration, Dedicated Account Manager, Priority Support (24/7), SLA Guarantee, Custom Branding Options, and Training & Onboarding. The right column, titled 'Contact Our Sales Team', contains a form with fields for 'Full Name *', 'Work Email *', 'Phone Number *', and 'Company Name *'. Below the company name field is a note: 'Optional, but it helps our sales team size a plan and pricing for you before the first call.' There is also a 'Company Size' dropdown menu with a 'Select size' button. Below that is a section 'Tell us about your needs' with a text area for 'Expected volume, use cases, Time Line...'. At the bottom of the form is a 'Security Check: 26 - 17 + ?' field with a 'Enter the answer' prompt. A yellow 'Submit Inquiry' button is at the very bottom. A link 'Back to Pricing' is at the bottom right.

The Enterprise inquiry form — only name, email, and company are required.

Common points of confusion

Answers to the questions that come up most, gathered in one place rather than only where each one occurs in the walkthrough above.

? My username doesn't look like an email — can I still sign in with it?

Yes. The identifier field takes either your email or your username; type whichever one you registered with.

? What exactly does GSTIN need to look like?

Fifteen characters: a 2-digit state code, your 10-character PAN, a 1-digit entity code, the letter Z, then a checksum character — e.g. 22AAAAA0000A1Z5. It's entirely optional; leave it blank unless you need GST invoices.

? I lost my authenticator app and my backup codes. Now what?

There's currently no self-service recovery for this — contact your organization's administrator. This is exactly why the backup codes are worth saving somewhere durable the moment they're shown.



Is the CAPTCHA on the register/login forms actually secure?

Today it's a math question, which stops unsophisticated bots. Once an administrator configures Cloudflare Turnstile, every one of these forms switches over automatically — no visible change to the workflow, just a stronger check.



My bulk upload was rejected for being too large, but each file is small — why?

The 500MB limit is for the whole batch's request size, not any single file. Split a large batch into two or more uploads instead of shrinking individual files.



If I lower the team's retention period, does old evidence get deleted right away?

No — changing it only updates the computed eligibility date going forward. Nothing on this platform is ever deleted automatically, regardless of this setting.



I created a webhook and now I can't find the secret anywhere — did it get lost?

It was shown once, in full, in the confirmation message right after creation. If it wasn't copied then, delete the webhook and add it again to get a new one — the platform can't show you the same secret twice.



What's the difference between a "Case" and a certificate?

A case is a container — it groups related evidence records (and their certificates) under one chain of custody for a single legal matter. It doesn't certify anything by itself.



I'm not a notified Section 79A Examiner — can I still complete Part B?

Yes. Choose "Not claimed" for Section 79A status and fill in your qualifications, certifications, and relevant experience instead, so the court can assess your expertise directly — this follows the Supreme Court's 2026 ruling that unnotified experts aren't barred from giving this opinion.

This handbook reflects the build current as of this writing. Screens change as the product does — if something here no longer matches what you see on screen, the in-app ? tips and field hints are the source of truth.