KADERNANI & COMPANY · AI LEGAL ASSISTANT

Legal AI
Administrator Guide

Managing users, access, matters, the audit trail and email for your firm

---

Version 2 · September 2026 · For firm administrators

Companion to the *Legal AI User Guide*, which covers day-to-day use. This guide covers only what the **Admin** role adds. Server configuration (hosting, AI model, mail connection) is handled by the service provider and is outside this guide.

Contents

1. The administrator role

An administrator is an ordinary user with the **Admin** flag switched on. Administrators see an extra **Admin** button in the top bar which opens three tabs: **Users**, **Usage** and **Audit**. They can also manage the membership of any matter, including restricted ones.

What administrators can do

- Create users, edit their name, role, initials and email, make them administrators, deactivate and reactivate them, reset their passwords.
- See usage statistics for every user and module.
- Read and export the firm's complete audit trail.
- Add or remove members of any matter, change a matter's access (firm-wide / restricted), close or reopen matters.
- Delete any vault document.
- Send a test email to check the mail connection.

What administrators cannot do

- **Read restricted matters they are not a member of.** They see the matter's name and can manage who is inside the wall, but the conversations, documents, client name, reference and parties stay hidden. This is deliberate — an ethical wall that administrators could bypass would not be a wall.
- Read other users' conversations. Conversations are private to their author; administrators see that they exist (in usage and audit) but not their content.
- Delete or alter audit entries.
- Deactivate their own account or remove the last remaining administrator.
- See the AI service costs. Usage shows volumes only; costs are managed by the service provider.

> **RECOMMENDATION**
>
> Have at least two administrators, and give the flag only to people who need it. Every administrative action is logged with the administrator's name and IP address.

2. First-day checklist

- ☐ Sign in with the administrator account provided to you and **change its password** (click your name → Change Password).
- ☐ Add **your email address** on your profile (click your name → Email Address → Save). Password resets and the test email depend on it.
- ☐ Admin → Users → **Send test email to me**. If it fails, tell the service provider — nothing else depends on you here.
- ☐ Create a second administrator.
- ☐ Create the users (section 3), one per person, each with their own email address. Do not share accounts — the audit trail is only meaningful with individual logins.
- ☐ Ask each user to sign in, change the initial password, and confirm their email on their profile.
- ☐ Decide the firm's matter conventions: naming (e.g. *Client* — *Subject*), who creates matters, and which kinds of matters must be restricted (section 4).
- ☐ Create the first matters or let the lawyers do it, and add adverse parties so conflict checks work from day one.
- ☐ Agree who reviews the audit trail and how often (section 6).

3. Users

Open **Admin** → **Users**. The form at the top creates users; the table below manages existing ones.

Creating a user

FIELD	NOTES
Username	3–50 characters: lower-case letters, digits, dot, underscore, hyphen. Used to sign in; cannot be changed later. Convention: `firstname.lastname`.
Full name	Shown in the top bar, in exports ("Prepared by"), in matter membership and in the audit trail.
Role / title	Free text, e.g. Partner, Associate, Paralegal. Descriptive only — it grants no permissions.
Email **(required)**	Must be unique. Used for password-reset links, as the Reply-To on emails the user sends from the system, and so colleagues can pick the person as an email recipient.
Initials	Up to 5 characters for the avatar; generated from the name if left blank.
Password	Minimum 8 characters. Give it to the person securely and ask them to change it on first sign-in.
Admin	Tick only for administrators.

Press **Add user**. The new account is active immediately.

Managing existing users

- **Admin switch** — grants or removes administrator rights. Removing your own rights asks for confirmation and closes the Admin panel. The last active administrator cannot be demoted.
- **Active switch** — off means the person cannot sign in. Their conversations, documents and audit history are kept and remain visible to matter members as before. Use this for leavers (section 8) rather than trying to delete accounts — accounts are never deleted, so the audit trail stays complete.
- **Name, role, initials (pencil beside the name)** — correct a person's details; the change shows immediately in exports and the audit trail.
- **Email (pencil beside the address)** — set or correct the person's address.
- **Reset password** — set a new password for the person (they should change it afterwards). Prefer letting users reset their own through *Forgot password?* on the sign-in screen when they have an email on file.

> **USERNAMES**
> The username cannot be changed after creation. If someone's name changes, update the full name; the username stays as their sign-in identifier.

4. Access control

How access works

- Every conversation is private to the user who created it. Users cannot open each other's conversations.
- Vault documents are shared within a matter: anyone who can see the matter can use its documents.
- A matter is **firm-wide** (all active users) or **restricted** (members only). Restriction hides the matter's conversations, documents and details from everyone else — including administrators who are not members.
- Within a matter, a **lead** can edit it, close/reopen it, change its access and manage members; a **member** can work in it. The creator is the first lead.

Managing a matter's membership

1. Left panel → **Manage** (Matters).
2. Find the matter. Restricted matters you are not a member of show *no access* — you still get the Members button.
3. Click the people icon. Add a person from the directory as Member or Lead; promote/demote with **Make lead** / **Demote**; remove with ×. Removal takes effect immediately.
4. Change **Access** between firm-wide and restricted in the same panel. Restricting a matter re-adds its creator as lead so nobody is locked out.

> **ETHICAL WALLS**
> Use restricted matters whenever the firm acts in a matter where some staff must be screened (conflicts cleared by consent, confidential transactions, internal investigations). Add adverse parties to every matter so the conflict check catches later clashes, and treat a *Conflict* result during matter creation as a compliance event: the acknowledging lawyer's note is in the audit trail under `matter.create`.

Closing matters

Closing a matter keeps everything readable and stops new conversations under it. Reopen when work resumes. Closing does not delete anything.

Deleting documents

Administrators, matter leads and the uploader can delete a vault document (bin icon in the Vault). Deletion removes the file from every conversation it was attached to and is logged; the record of the document's existence and history stays in the audit trail.

5. Usage

Admin → Usage shows, for the last 7 to 365 days and optionally one user: requests, input and output tokens, cache reads, official-source web searches, a daily chart, and tables per user and per module.

Reading it

- **Requests** — every question or follow-up sent to the AI.
- **Input / output tokens** — a measure of how much text went in (including attached documents) and came out. Roughly 750 words per 1,000 tokens.
- **Cache reads** — document context reused from a previous turn (cheaper and faster); a high share means the vault is being used well.
- **Web searches** — checks against official UAE sources. Each user has a daily allowance; the AI tells the user when it is reached.

Use the per-user table to see adoption and to spot accounts that are never used (candidates for deactivation) or unusually heavy (worth a conversation about how they work). Cost figures are not shown; the service provider reports them.

6. The audit trail

Admin → Audit. The audit log is **append-only**: entries cannot be edited or deleted from the application, by anyone.

What is recorded

ACTION	MEANING
`login`, `login.failed`, `logout`	Sign-ins, failed attempts (with the username tried) and sign-outs.
`conversation.create / open / delete`	A conversation started, reopened (with the documents attached at the time) or deleted.
`ai.request`	A question sent to the AI: module, model, the IDs of the documents transmitted, web searches run. This is the firm's record of what left the system for processing.
`document.upload / download / delete / attach / detach / email`	Every touch of a vault document, with its name and, for emails, the recipients.
`matter.create / update / close / reopen / member_add / member_remove`	Matter lifecycle and membership changes; *create* includes any acknowledged conflicts and the clearance note.
`access.denied`	An attempt to reach a restricted matter or its documents by a non-member.
`export.pdf / export.docx / export.copy / export.email`	Answers saved, copied or emailed (with recipients).
`password.reset_request / reset_complete / reset_invalid / reset_throttled`	Self-service password resets, including expired or forged links and rate-limited attempts.
`profile.update`, `admin.user_create / user_update / password_reset`, `audit.export`, `email.test / email.failed`	Profile and administrative actions; audit exports; mail test results and failures.

Each entry carries the time, user, action, the matter it relates to, details, the IP address and browser.

Using the filters

Filter by period, user, action (a whole family such as `document.*` or a single action), matter, or free text (matches usernames, details and IP addresses). **Export CSV** downloads the filtered set (UTF-8, opens in Excel) — the export itself is logged.

Suggested routine

- **Weekly**: filter `login.failed` and `access.denied` — repeated failures from one IP or one user deserve a question.
- **Monthly**: review `export.email` and `document.email` for sends outside the firm's domain; review `matter.create` entries with acknowledged conflicts.
- **On request** (client audit, regulator, dispute): filter by matter and export.
- **Per matter**: leads and members can see their own matter's activity from Manage Matters → Activity, without needing the Admin panel.

7. Email

Email lets users send answers and vault documents as attachments and lets everyone reset a forgotten password themselves. The mail connection is configured by the service provider; your part is to test it and to keep users' email addresses complete.

Testing

Admin → Users → Send test email to me. You need an email on your own profile. A failure message names the cause (connection, authentication, rejected sender); pass it to the provider.

How messages appear

- Emails a user sends show "*Their Name via Legal AI*" as sender, from the firm's system address, with **Reply-To** set to the user's own email — so replies go to the lawyer, not the system.
- System emails (password resets, tests) come from the system address only.
- Every email carries a confidentiality and AI-review notice.
- Sending outside the firm asks the user to confirm; the provider can restrict sending to the firm's own domains if you prefer.

Supporting a password reset

If a user cannot use *Forgot password?* (no email on file, link expired, more than three requests in an hour), set their email in the Users tab and ask them to try again, or use **Reset password** directly.

8. Joiners, movers and leavers

Joiner

- ☐ Create the user with their firm email; tick Admin only if needed.
- ☐ Add them to the restricted matters they will work on (Manage → Members).
- ☐ Send the *User Guide*; ask them to change the initial password and confirm their email.

Mover (change of team or matter)

- ☐ Remove them from restricted matters they must no longer see; add them to the new ones. Both are immediate and logged.
- ☐ If they become a lead, promote them in the matter; ensure the matter keeps another lead if they later leave.

Leaver

- ☐ Switch **Active** off the day they leave (they can no longer sign in; nothing is deleted).
- ☐ Remove them from restricted matters if you want the membership lists to reflect current staff (not required for security — an inactive user cannot sign in).
- ☐ If they were the only lead of any matter, promote another member first.
- ☐ If they were an administrator, make sure at least one other administrator remains, then switch Admin off.
- ☐ Their conversations and uploaded documents remain available to matter members; the audit trail keeps their history.

9. Security practices

- **One person, one account.** Never share logins; shared accounts make the audit trail meaningless and break ethical walls.
- **Passwords**: minimum 8 characters is enforced; ask for 12+ with a passphrase. Reset any password you have communicated in writing.
- **Administrators**: as few as possible, at least two, reviewed quarterly.
- **Restricted matters** for anything conflict-cleared by consent, market-sensitive, or involving staff members personally.
- **Adverse parties** recorded on every matter, including individuals, so conflict checks work.
- **External email**: remind users that sending a document outside the firm is logged and asks for confirmation; consider domain restriction with the provider.
- **Devices**: sign out on shared computers; sessions expire after eight hours anyway.
- **Audit review** on a fixed schedule (section 6) with a named owner.
- **Data handling**: uploaded documents are stored in the firm's vault on the firm's hosting and are transmitted to the AI service for each request that uses them; deleted documents are removed from storage. Ask the provider for the current data-residency statement before promising clients anything in writing.

10. Troubleshooting and quick reference

SITUATION	ACTION
User cannot sign in	Users tab: is **Active** on? Reset the password, or have them use *Forgot password?* (needs an email on file).
"Forgot password" says email is not available	The mail connection is off — contact the provider; reset the password manually meanwhile.
User says a matter has disappeared	It is restricted and they are not a member, or it was closed and they filtered on open matters. Check Manage Matters.
Conflict acknowledged wrongly	Nothing is undone automatically. Edit the matter's parties, restrict or close it as appropriate, and note the correction — the audit trail keeps both events.
Need to prove who saw a document	Audit → filter action `document.` and the matter → Export CSV. Note that opening a conversation lists the documents in context at that time (`conversation.open`).
Suspicious sign-in attempts	Audit → `login.failed`, look at IP and username; reset the affected password; inform the provider if it continues.
Test email fails	Send the exact error to the provider; check your own profile has an email address.
Wrong name or role on a user	Admin → Users → pencil beside the name.

Quick reference

TASK	WHERE
Create a user	Admin → Users → form at the top
Deactivate / reactivate	Admin → Users → Active switch
Make / remove an administrator	Admin → Users → Admin switch
Reset a password	Admin → Users → Reset password
Set a user's email	Admin → Users → pencil beside the email
Correct a name, role or initials	Admin → Users → pencil beside the name
Add / remove someone from a matter	Left panel → Manage → people icon
Restrict or open a matter	Manage → people icon → Access
Close / reopen a matter	Manage → archive / tick icon
See usage	Admin → Usage
Investigate or export activity	Admin → Audit → filters → Export CSV
Test the mail connection	Admin → Users → Send test email to me