ELLM

The Audit Log in the eLLM Admin Console

The audit log is a complete, searchable record of activity in eLLM. Administrators use it to investigate specific events, answer compliance questions, and export records. This article explains what is recorded and how to use the log.

AUTHOR
Paul Flanders

PUBLISHED
4 Jun 2026

DOCUMENT
InfoHub — Knowledge, news, and updates from EssingtonITS

The Audit Log in the eLLM Admin Console

Paul Flanders · 4 Jun 2026

What this product is for

For trust and compliance, you need to know what happened and when. eLLM records every query, document upload, login, and administrative action. The audit log lets administrators search that record, look at the detail of any event, and export results for reporting.

Main features

- A filterable browser over all recorded activity.
- Filter by event type, user, or date range.
- View the full detail of any event.
- A **Model** column showing which model answered each query.
- Export filtered results as a CSV file for compliance reporting.

How to use it

Browsing the log

1. Sign in to the admin console and open the **Audit** section.
2. Use the filters to narrow the list by event type, username, or date range.
3. Select an entry to see its full request and response detail.

Exporting records

1. Apply the filters you want so the list shows the relevant events.
2. Export the filtered results as a CSV file.
3. Open the file in a spreadsheet for reporting or to share with auditors.

Common tasks

- **Investigate a specific query:** filter by the user and date, then open the entry.
- **See which model answered:** check the Model column.
- **Produce a compliance report:** filter to the period and export to CSV.
- **Review logins or uploads:** filter by event type.

Things to know

- The audit log is append-only. The application never deletes entries.
- Every query records which model pool answered it, alongside the rest of the event detail.
- Activity through the external API is also recorded, identified by the API key that made the request rather than a person.
- Because it is a full record, the audit log is the most reliable source when investigating what actually happened.

Troubleshooting

- **I can't find an event:** widen the date range and check the event-type and username filters.
- **The export is very large:** apply tighter filters before exporting to keep the file manageable.

- **An event shows an API key rather than a person:** that request came from an external service using its key, which is expected.

Frequently asked questions

What gets recorded?

Queries, document uploads, logins, and administrative actions, each with detail.

Can entries be deleted?

No. The log is append-only and the application does not remove entries.

How do I know which model answered a query?

The Model column shows the pool that produced each answer.

Can I share results with auditors?

Yes. Filter to what you need and export as a CSV file.

Summary

The audit log is eLLM's trustworthy record of activity. Administrators filter it by type, user, or date, open any event for full detail, see which model answered each query, and export results for compliance. Because it is append-only, it is a dependable account of what happened.

> Need assistance navigating the complexities of eLLM? EssingtonITS offers expert guidance and tailored IT solutions to help you succeed. Visit EssingtonITS.co.uk for comprehensive support.