Permissions, export and privacy

Mail Log stores potentially sensitive communication data. This page sums up who may do what, what is exported and which data is stored at all.

Permissions

You assign the permissions as with every Joomla component under *Options* → *Permissions* per user group. Mail Log deliberately separates viewing from reading the content:

Permission	Allows
View Mail Log	Open the dashboard and the list — the metadata, but not necessarily the message texts.
View mail content	Read the full bodies (HTML, text, MIME). Granted separately because bodies can contain sensitive data.
Download attachments and .eml	Download attached files and the raw message.
Resend mails	Deliver logged mails again.
Delete entries	Remove log entries.
Manage demo data	Create and delete test entries.

> Every action checks its permission server-side — it is not just the interface hiding buttons. So an action cannot be forced through a direct call either. An editor with "view Mail Log" but without "view mail content" sees the list but no texts.

Recommendation: grant *view mail content* and *download attachments and .eml* sparingly — ideally only to the people who actually investigate delivery problems.

Export

The button *Export CSV* in the list outputs the currently filtered selection as a CSV file. The export contains ID, time, status, sender, recipient, subject, source, context and the error message — but **not** the message text. Whoever needs bodies opens the entry or downloads the .eml file (with the corresponding permissions).

> Free-text fields are prepared in the CSV so that spreadsheet programs do not interpret them as a formula by accident. The export can therefore be opened safely in Excel or LibreOffice.

Which data is stored

Per mail, Mail Log stores sender and recipients, subject, time and status, the context as well as — where available — the IP address and the user ID of whoever triggered it. How much of the text is kept is up to you through the storage mode; out of the box that is a short excerpt only, and sensitive mails are stored with metadata only.

Privacy notes for operation

- **Limit retention.** Set an entry retention (default 180 days) and set up the cleanup task, so that old data does not lie around indefinitely.
- **Store frugally.** For most purposes the default "metadata + excerpt" is enough. Full or raw storage only if you really need it.
- **Encrypt if you keep full bodies.** Encrypted storage keeps the key outside the database.
- **Keep permissions narrow.** Separate reading the content from merely viewing the list.
- **Access and erasure requests.** For data subject requests, filter the list by the address and export or delete selectively.

All data stays on your server — Mail Log contacts no external services.

Applies to version 1.5.0.

Deutsche Fassung

Revision #11
Created 2026-08-16 13:09:21 UTC by Norbert Graup
Updated 2026-10-27 22:55:09 UTC by Norbert Graup