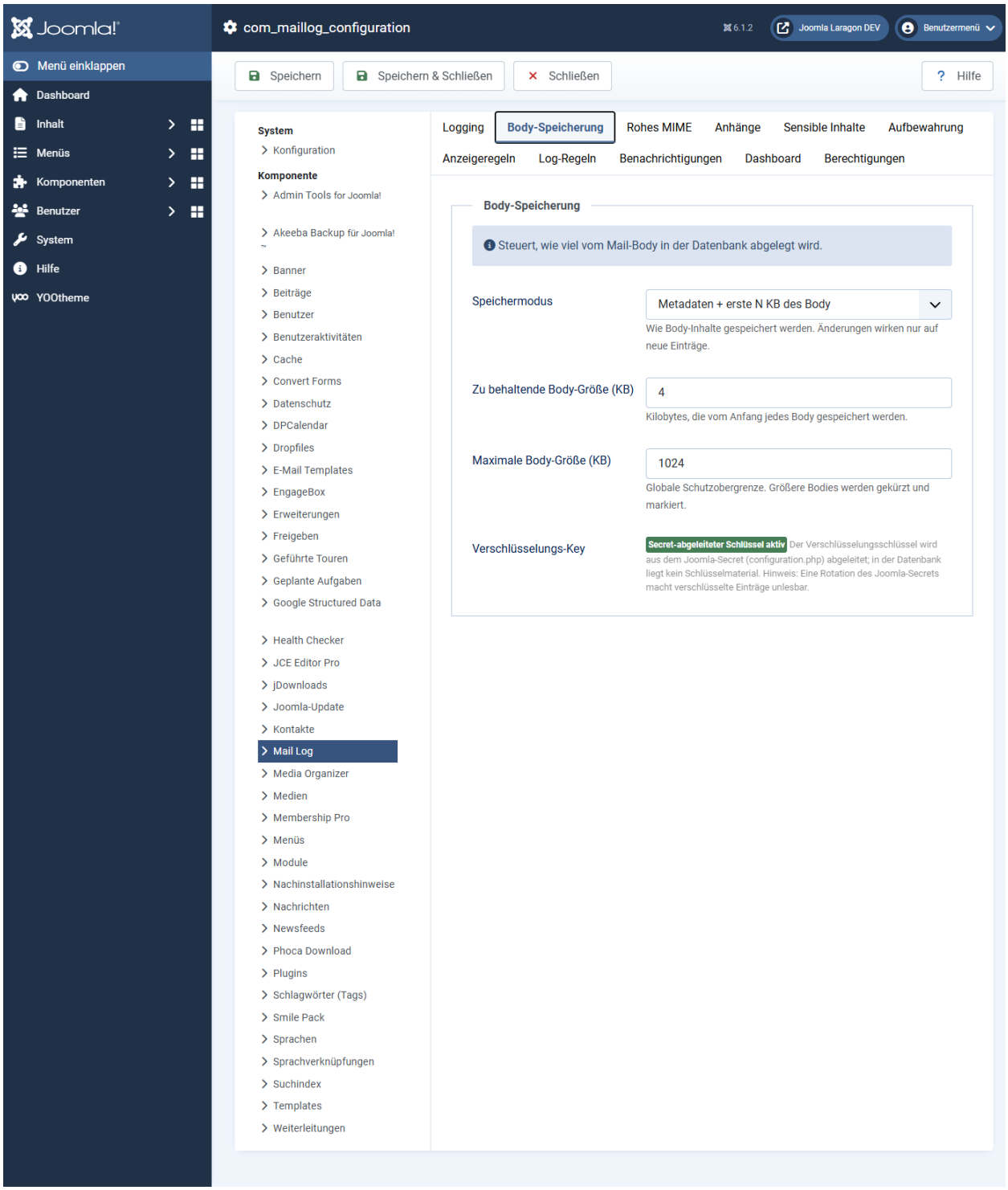
Body-Speicherung, Verschlüsselung und sensible Inhalte

Wie viel vom Nachrichtentext Mail Log speichert, entscheiden Sie selbst. Diese Seite erklärt die Speichermodi, die Verschlüsselung und die Sonderbehandlung sensibler Mails. Alle Einstellungen finden Sie in den *Optionen* unter den Reitern *Body-Speicherung*, *Rohes MIME* und *Sensible Inhalte*.

> Änderungen am Speichermodus wirken nur auf **neue** Einträge. Bereits gespeicherte Mails bleiben, wie sie sind.

Die Speichermodi für den Body



Der Reiter *Body-Speicherung* steuert, wie viel vom Text abgelegt wird.

Modus	Was gespeichert wird
Metadaten + erste N KB *(Voreinstellung)*	Nur die ersten Kilobytes des Texts. Reicht für einen Eindruck, ohne lange Nachrichten vollständig abzulegen. Die Größe stellen Sie mit *Zu behaltende Body-Größe (KB)* ein (Standard 4 KB).
Vollständiger Body	Der komplette Text im Klartext.

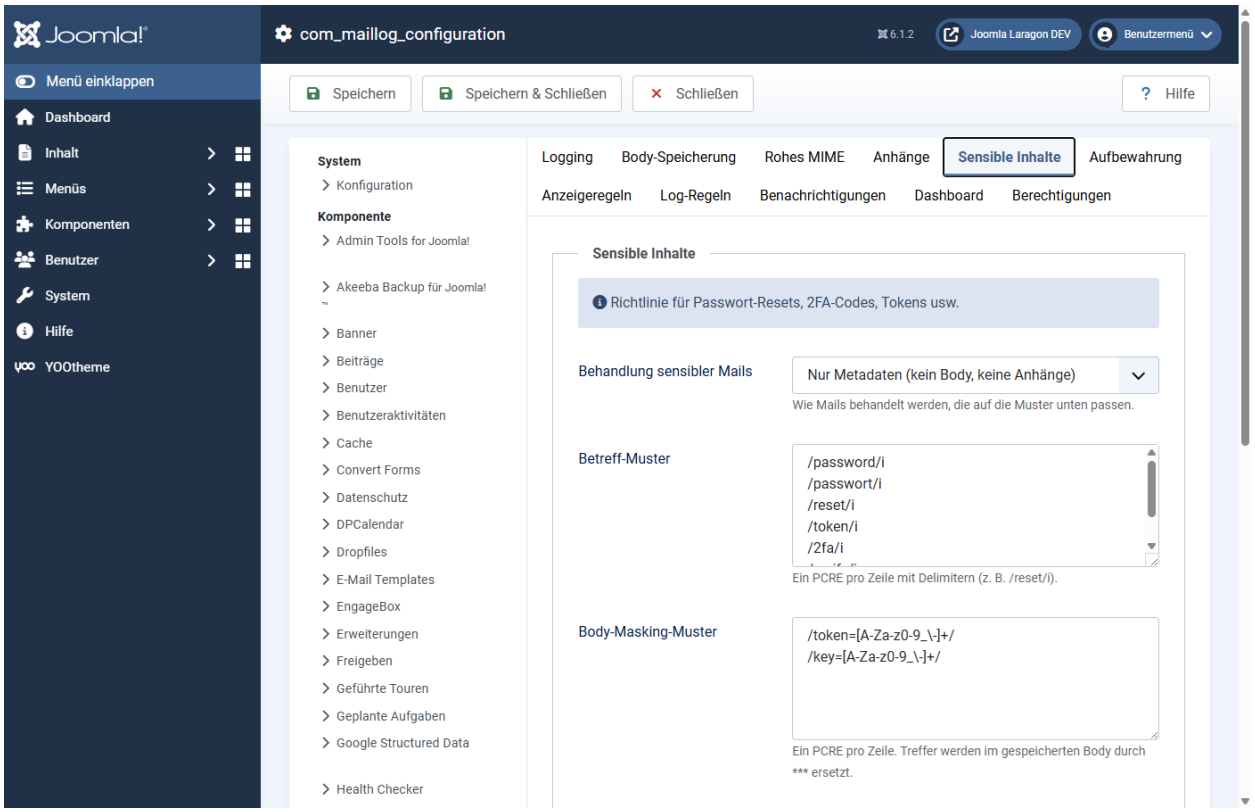
Modus	Was gespeichert wird
Vollständig, verschlüsselt	Der komplette Text, verschlüsselt in der Datenbank (siehe unten).
Vollständig, automatisches Löschen nach N Tagen	Der komplette Text, aber der Wartungs-Task entfernt ihn nach der eingestellten Frist wieder und behält nur die Metadaten.
Nur Metadaten	Gar kein Text — nur Absender, Empfänger, Betreff, Status und Zeit.

Zusätzlich begrenzt *Maximale Body-Größe (KB)* als globale Schutzobergrenze jeden Text; größere Bodies werden gekürzt und in der Detailansicht als gekürzt markiert.

Rohes MIME

Unabhängig vom Body-Modus können Sie im Reiter *Rohes MIME* die exakte, wie versendet aufgebaute RFC822-Nachricht speichern. Das ermöglicht saubere **.eml**-Downloads für ein Audit. Weil das rohe MIME den vollständigen Klartext enthält, ist diese Option **ab Werk ausgeschaltet**. Sie lässt sich ebenfalls verschlüsseln.

Verschlüsselung



Der Reiter *Sensible Inhalte* mit den Betreff- und Masking-Mustern.

Verschlüsselte Bodies und MIME-Nachrichten schützt Mail Log mit einem modernen Verfahren (AES-256-GCM bzw. XChaCha20-Poly1305). Entscheidend ist die Herkunft des Schlüssels:

> Der Schlüssel wird aus dem **geheimen Joomla-Schlüssel** (in Ihrer `configuration.php`) abgeleitet und liegt **nicht in der Datenbank**. Ein Angreifer, der nur die Datenbank erbeutet, kann die Inhalte deshalb nicht entschlüsseln.

> Kehrseite: Ändern Sie den geheimen Joomla-Schlüssel, lassen sich zuvor verschlüsselte Einträge nicht mehr lesen. Der Schlüssel gehört zum ohnehin schützenswerten Kern Ihrer Joomla-Installation — behandeln Sie ihn entsprechend.

Das Feld *Verschlüsselungs-Key* in den Optionen ist seit dieser Version eine reine **Statusanzeige**. Sie müssen nichts eintragen oder erzeugen. Zeigt es einen „Alt-Schlüssel", stammt er aus einer früheren Version; der Wartungs-Task *Alt-verschlüsselte Bodies migrieren* stellt solche Einträge auf das neue Verfahren um und entfernt den Alt-Schlüssel danach selbst.

Sensible Mails

Manche Mails sollten nie im Klartext im Log landen — Passwort-Resets, Bestätigungslinks, Einmal-Codes. Mail Log erkennt sie an der Betreffzeile und behandelt sie gesondert.

Im Reiter *Sensible Inhalte* stehen dafür zwei Musterlisten (je ein regulärer Ausdruck pro Zeile) und eine Richtlinie:

Betreff-Muster	Passt der Betreff auf eines der Muster, gilt die Mail als sensibel. Ab Werk sind Muster für `password`, `passwort`, `reset`, `token`, `2fa`, `verify` und `verifizier` hinterlegt.
Behandlung sensibler Mails	*Nur Metadaten* (Voreinstellung, kein Body, keine Anhänge), *Normal protokollieren* oder *Gar nicht protokollieren*.
Body-Masking-Muster	Zusätzliche Muster, deren Treffer im gespeicherten Text durch `***` ersetzt werden — etwa `token=…` oder `key=…`.

Mit den Voreinstellungen landet ein Passwort-Reset-Link also nicht im Log, ohne dass Sie etwas einrichten müssten.

Gilt für Version 1.0.4.

Revision #6
Created 2026-07-30 17:11:45 UTC by Norbert Graup
Updated 2026-08-12 11:29:46 UTC by Norbert Graup