

File Upload

Package manual · Secure frontend upload of images, videos and documents for logged-in users (module) plus backend management (component) – Joomla 5/6

1. Overview

The **File Upload** package is the successor to "Image Upload" and installs two building blocks:

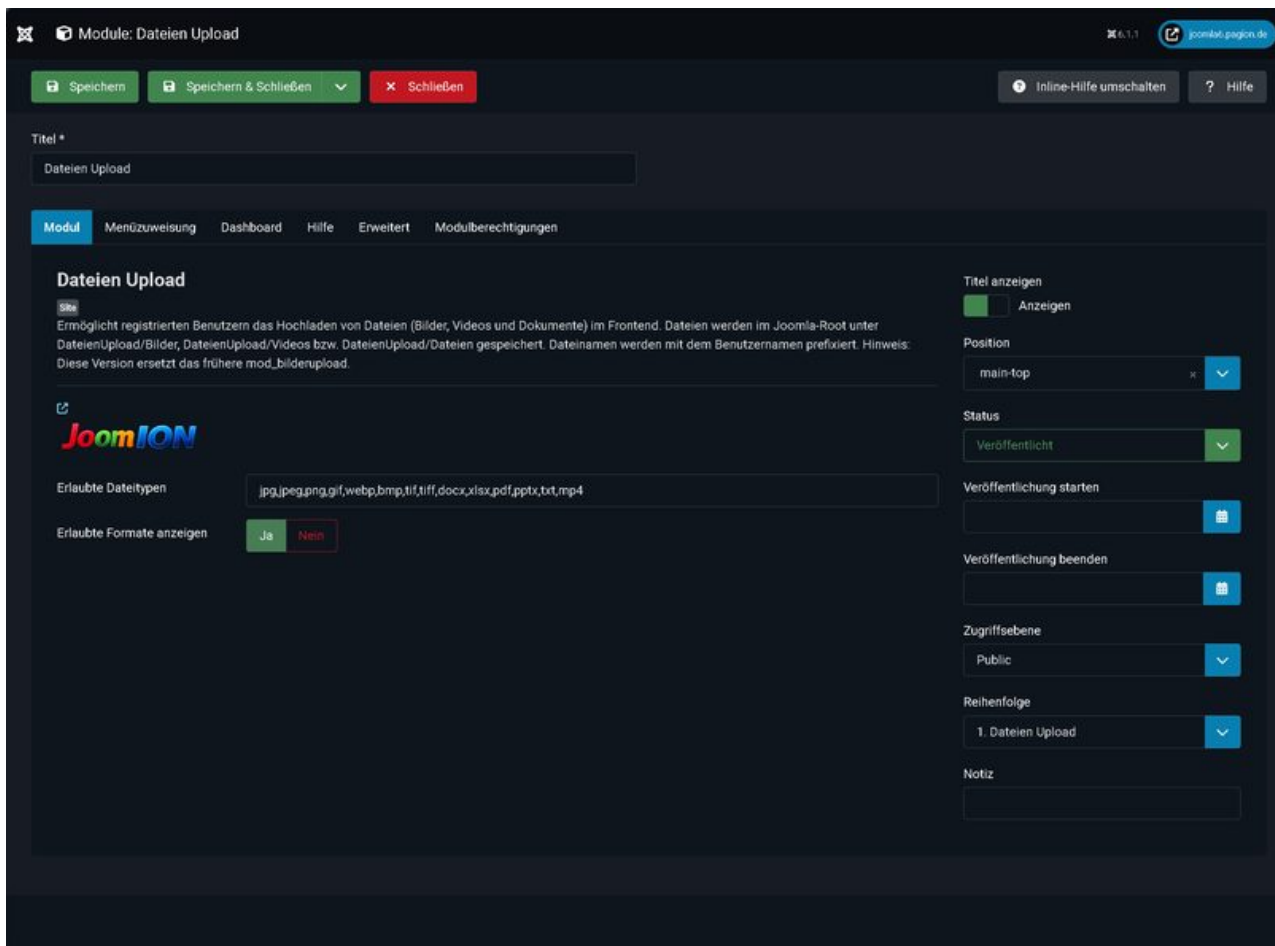
- **Module** ``mod_dateienupload`` (frontend): upload form for **logged-in** users.
- **Component** ``com_dateienupload`` (backend): management of the uploaded files – view, download (individually/ZIP) and delete.

Allowed are **images** (jpg, jpeg, png, gif, webp, bmp, tif, tiff), **videos** (mp4) and **documents** (pdf, txt, docx, xlsx, pptx). The files are stored separately by category:

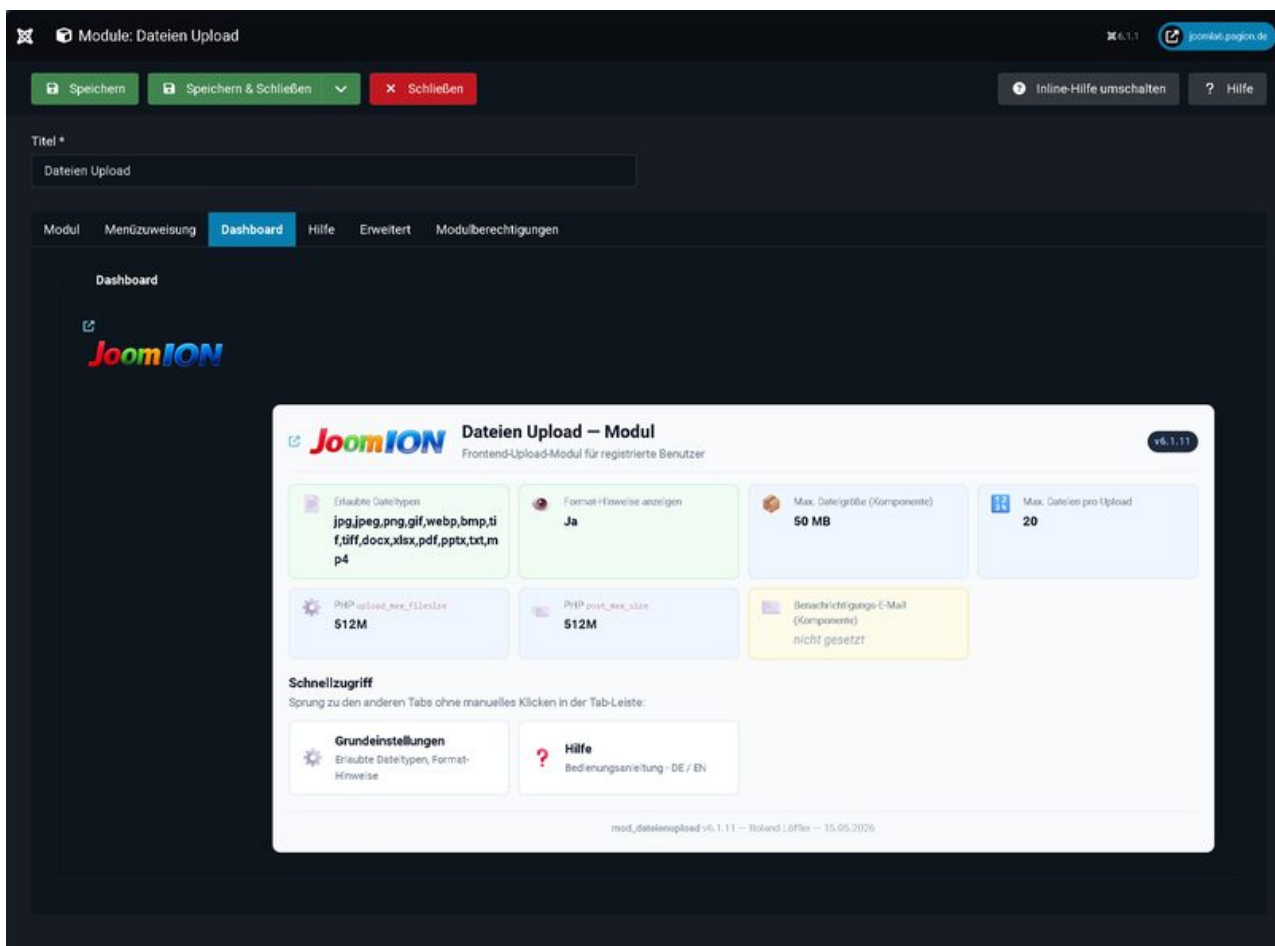
Category	Directory
Images	DateienUpload/Bilder/
Videos	DateienUpload/Videos/
Documents	DateienUpload/Dateien/

2. Installation

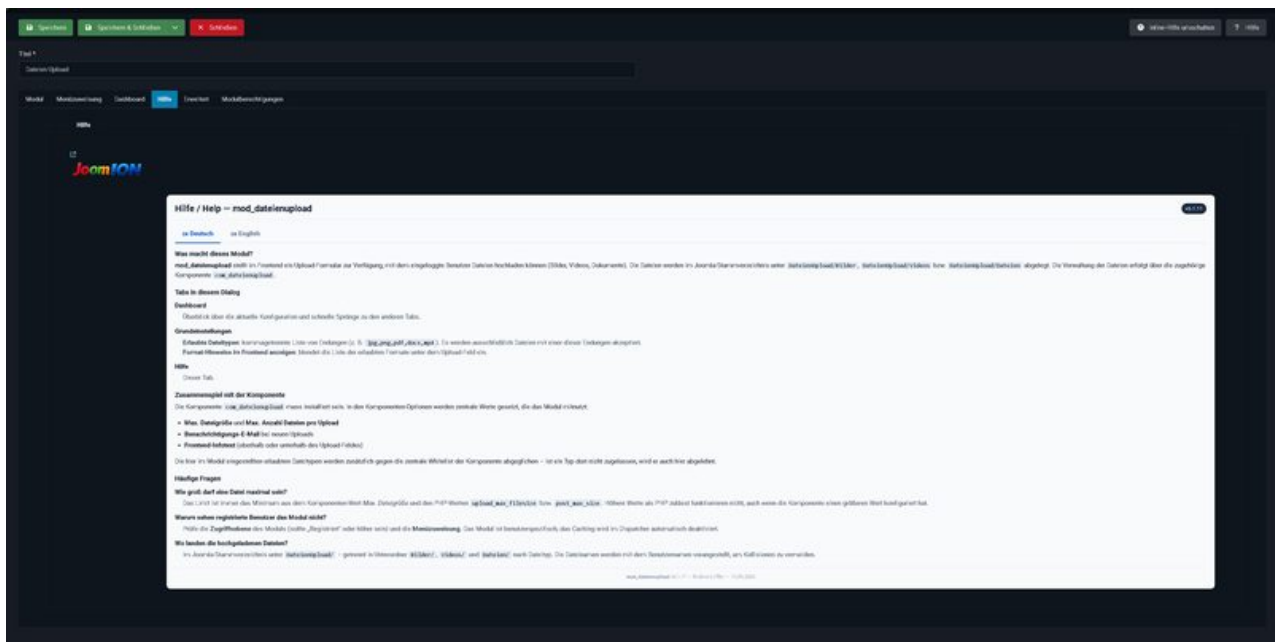
- 1 Upload the package `pkg_dateienupload-X.zip` via **System** → **Install** (component + module).
- 2 Under **Content** → **Site Modules** create a **"File Upload"** module, assign a position and publish it (access: logged-in users).
- 3 Open the backend management under **Components** → **File Upload**.



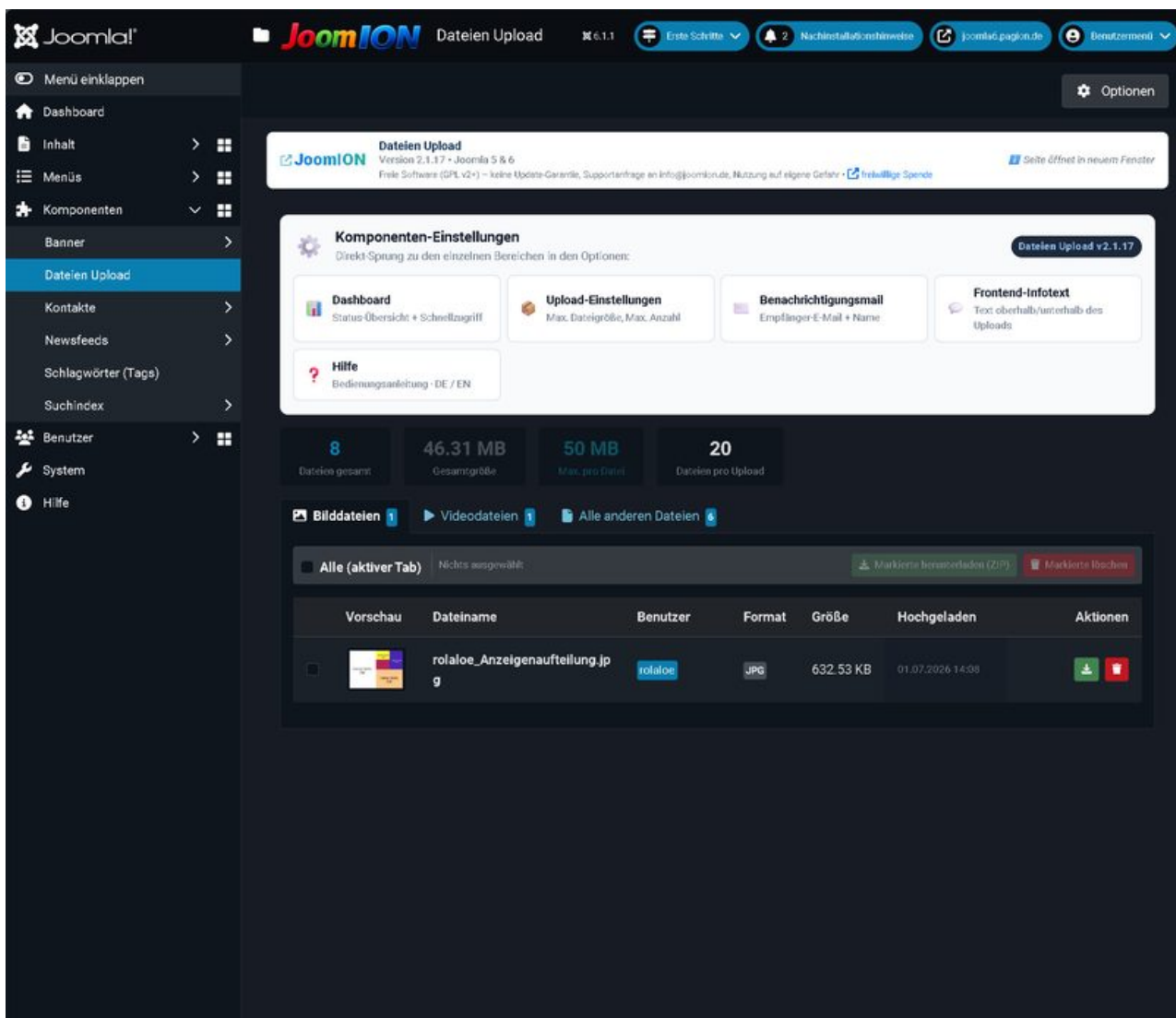
The "File Upload" module with the allowed file types



The built-in dashboard in the module editor



The module's built-in help page

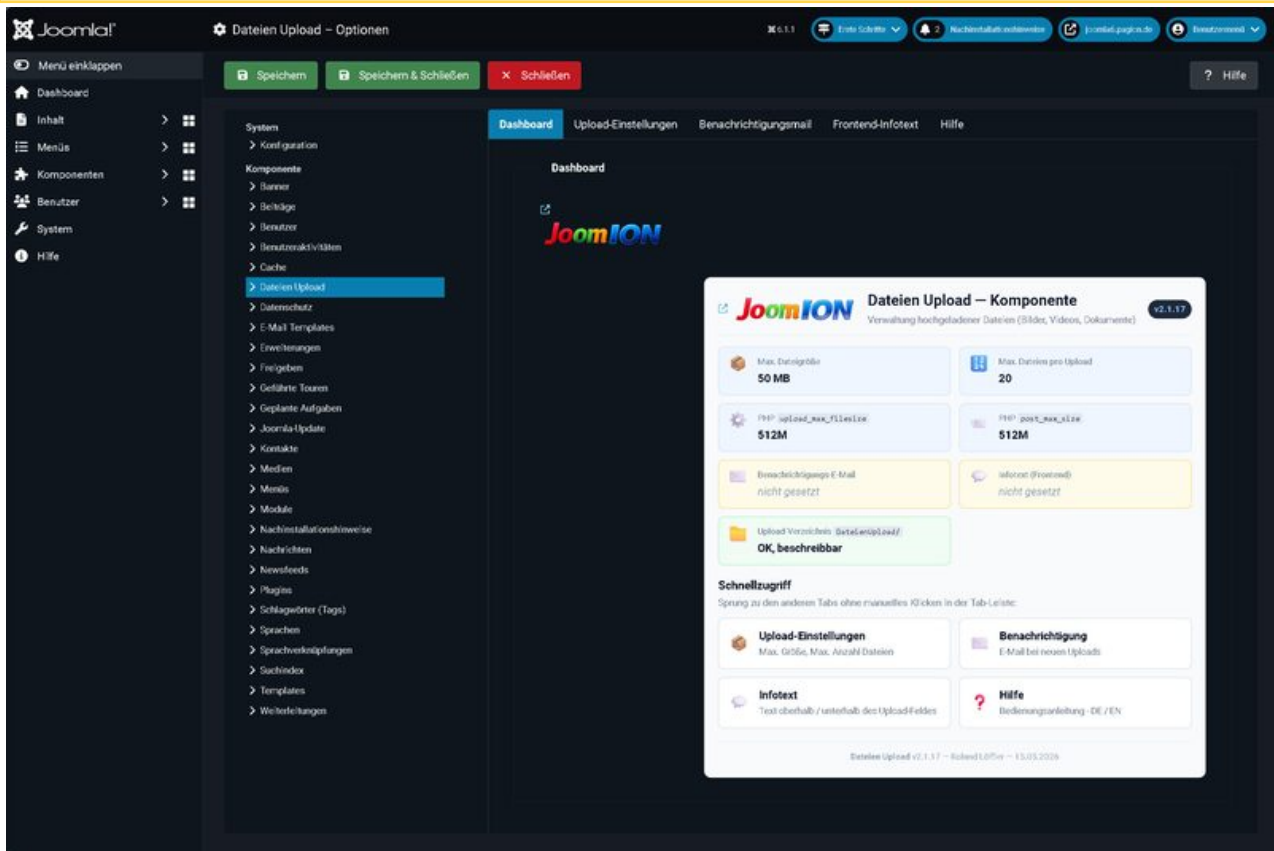


The "File Upload" backend management with dashboard and file list

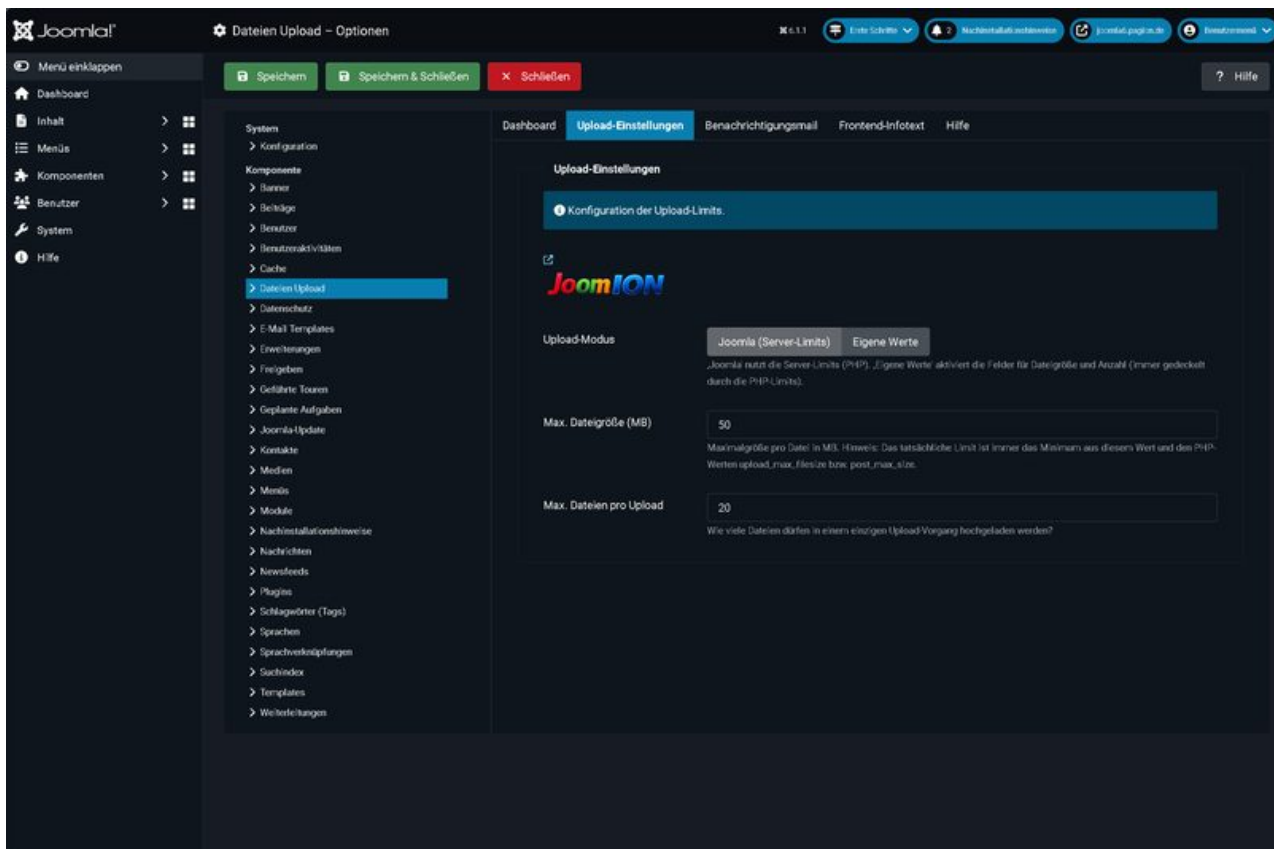
3. Settings (component options)

- **Upload limits:** maximum number of files per upload and maximum file size (MB).
- **Notification e-mail:** optional, with recipient address (fallback Joomla system mail).

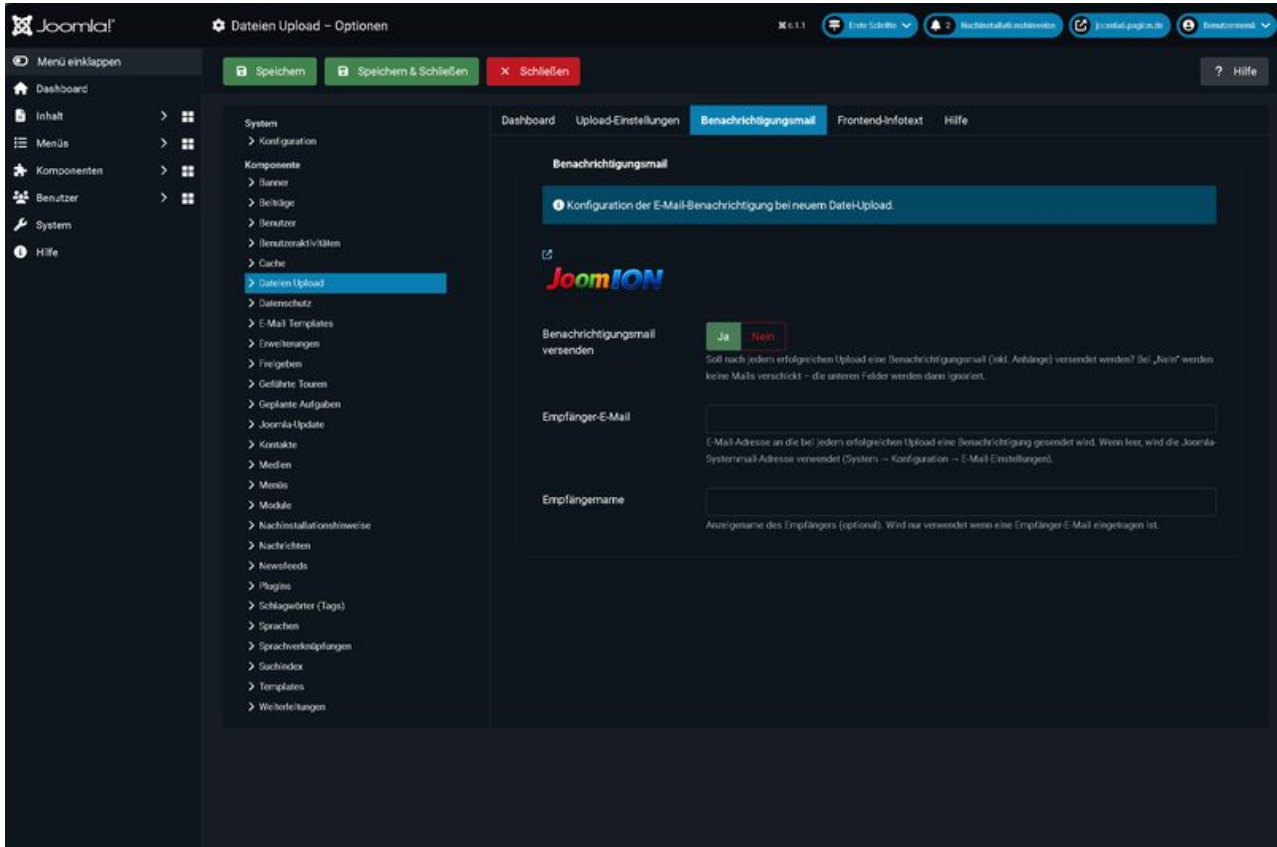
The server-side limits `upload_max_filesize` and `post_max_size` (php.ini/.htaccess) apply additionally and cannot be raised in PHP at runtime.



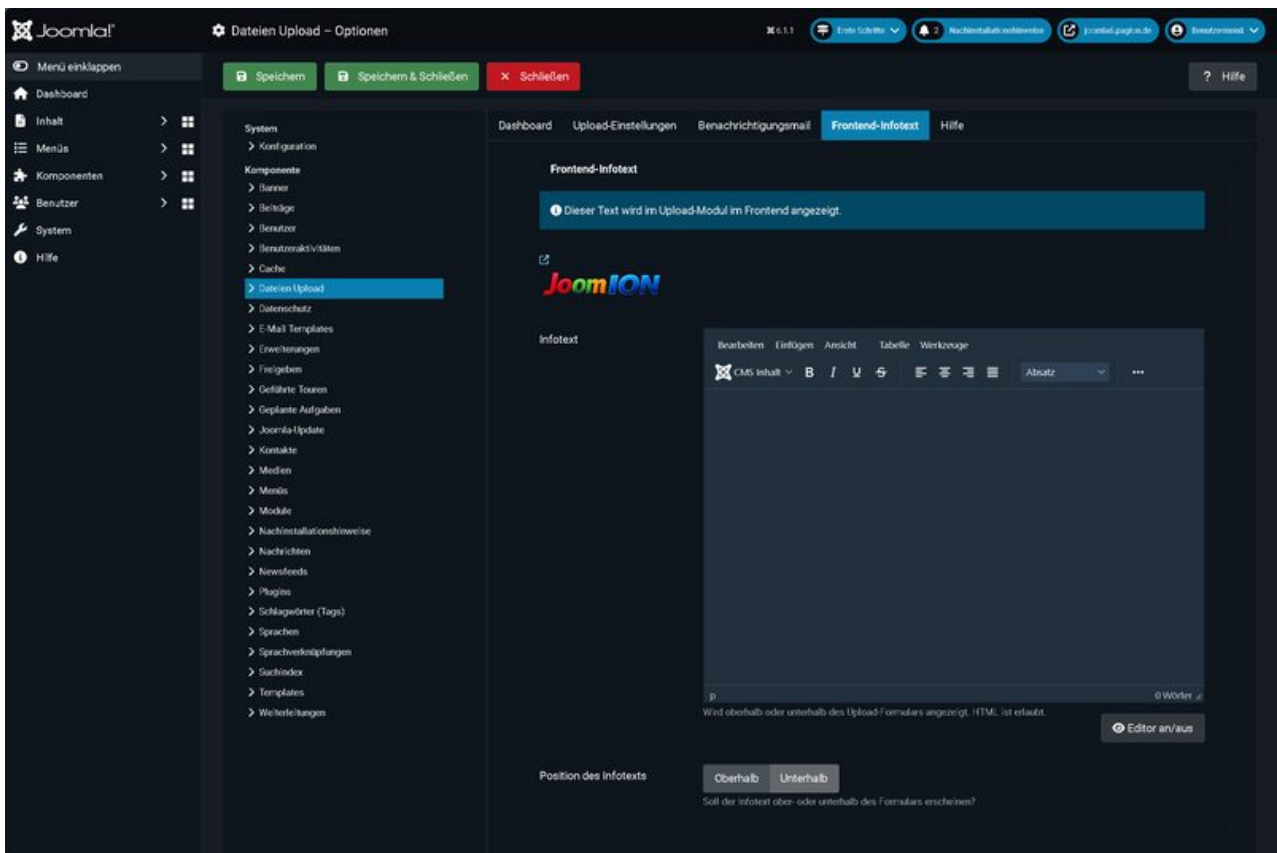
The component options dashboard



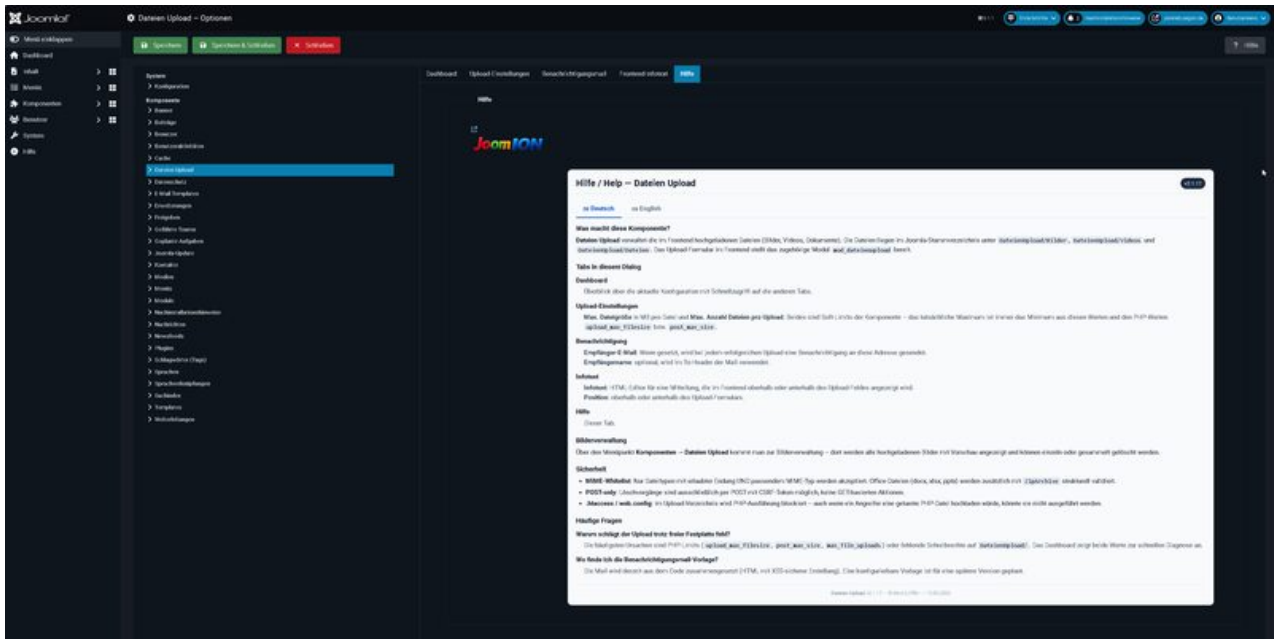
Upload settings (file size, count)



Notification e-mail settings



Frontend info text setting



The component's built-in help page

4. Security

The upload is secured several ways (defense in depth):

- **CSRF token** and **mandatory login** – no guest upload.
- ``is_uploaded_file()`` + ``move_uploaded_file()``.
- **MIME check via magic bytes** (`finfo`), not via the browser-supplied value; `application/octet-stream` is deliberately **not** allowed.
- **Office files** (docx/xlsx/pptx) are additionally validated by checking the **ZIP content** (e.g. `word/document.xml` must be present).
- **Whitelist** per category and a **hard blocklist** for executable/script/macro files – including double extensions like `file.php.pdf`.
- **File name sanitisation**, `basename()`, fixed permissions.
- **Delete/download** in the backend only via a `realpath()` check against the respective category directory (no path traversal/symlink), with token and `core.manage` permission check.

The package injects **no malicious code**: `_JEXEC` protection in all files, namespaced, Joomla 5/6 API. No `eval`/shell operations; database access with bound parameters.

5. Licence, updates & donations

Free software (GPL v2+). The package is free of charge and needs **no licence key**. **No update guarantee**, **no guaranteed support** – **use at your own risk**. Support requests are welcome at info@joomion.de.

Updates are delivered normally through the **native Joomla updater** (System → Update → Extensions) – without any licence check.

If this package helps you, a **voluntary donation** on joomion.de is appreciated. Thank you!

6. Frontend usage

- 1 Log in as a registered user and open the page with the upload module.
- 2 Select one or more files (image/video/document) and upload them.

- 3 After a successful upload a confirmation appears; optionally a notification e-mail is sent to the operator.